Dirk Engling
elektronische Problemlösungen

Dirk Engling, Gaudystraße 6 in 10437 Berlin

Kanzlei Hubrig
Gaudystraße 6
10437 Berlin

erdgeist@erdgeist.org
+49 163 741 84 42

Bankverbindung
DE34 **1007 0024** 0099 5027 00
DEUTDEDBBER

Steuernummer
31/277/64725
DE262231927

PGP-Fingerprint
68D0 5298 6E09 BF62 94B8
4DD0 B8DD 7017 **2A6C 30D3**

Berlin, 26. November 2015

Gegengutachten zu

- Gutachten 120222/04 vom 30. 03. 2012 –
  Gutachten über die sachgerechte Aufzeichnung von Torrent-Daten mit dem System “Observer”
- Stellungnahme 130319/04 vom 09. 04. 2013 –
  Ergänzungsgutachten zu Änderungen am System “Observer”
- Gutachten 141117/04 vom 17. 12. 2014 –
  Gutachten zur korrekten Ermittlung von IP-Adressen eines BitTorrent-Systems
- Gutachten 140801/04 vom 19. 08. 2014 –
  Ergänzungsgutachten zu Änderungen am System “Observer”
- Stellungnahme 1202424/04 vom 10. 05. 2012 –
  Stellungnahme über die Nachfrage des Gerichts bezüglich des Systems “Observer”

Des Sachverständigen-Büro für Computerwesen Prof. Dr. Pausch & Partner im Privatauftrag der GuardaLey Limited aus Leopoldshafen.

Dem Gegengutachter wurden von der Kanzlei Hubrig folgende Fragen zu den oben benannten Gutachten übermittelt:

1. Lassen die vorliegenden Gutachten genug Rückschlüsse auf Architektur und Implementierung der Software zu?
2. Wenn nein, welche Teile fehlen, sind diese für eine lückenlose Beweisführung essentiell?
3. Unter Vorbehalt der destillierbaren Informationen:
   3.1. Entsprechen Architektur und Implementierung der Software dem Stand der Technik?
   3.2. Worin unterscheidet sich die Software von der anderer Anbieter am Markt? Was sind Stärken und Schwächen?
4. Fand eine kritische Auseinandersetzung mit der begutachteten Software statt?

Fragen zu den Gutachten selbst:

1. Entsprechen die Gutachten qualitativen Anforderungen?
2. Kann eine Aussage getroffen werden, ob alle Fragen an den Gutachter korrekt beantwortet wurden?

Umfang des Gutachtens

Das vorliegende Privatgutachten dokumentiert die übergreifende Architektur der von der Firma GuardaLey Ltd. programmierten Projekts “Observer” zufriedenstellend. Über die Qualität der Implementierung und Zuverlässigkeit der Aussagen der Software lässt das Gutachten jedoch kaum Rückschlüsse zu. Die aus den Gutachten ableitbaren Sachverhalte über das Projekt “Observer” an sich werden im Punkt “Stand der Technik” zusammengefasst.

Aus den vorliegenden Ergänzungsgutachten lässt sich jedoch herleiten, dass mehrere Versionen der begutachteten Software existieren. Ferner schließt der Gutachter essentielle Fragestellung über die Umgebung des Systems aus, da sie nicht Teil des an ihn gerichteten Fragenkatalogs waren:

Zitat:

“Der Computer ist mit dem Betriebssystem Linux (die Art der Distribution sowie die Kernelversion waren nicht Bestandteil der Untersuchung) ausgestattet.”

“Hierbei wird die Untersuchung auf die Implementation des sog. Broker-Systems, hier auch Observer genannt, beschränkt.”

Um eine Beweisführung auf der von der Software gelieferten Ergebnisse aufzubauen, ist es jedoch unerlässlich, auch und gerade die Umgebung zu dokumentieren, in der das System betrieben wird. Besonders kritisch und absent sind dabei

- Auditierung der Softwaresicherheit und Zugangskontrolle zu den Systemen,
- die exakten Protokollierung der eingesetzten Versionen, beispielsweise durch:

- die Dokumentation der Übereinstimmung von übersetzter Software mit deren Quellcode (üblicherweise durch Prüfsummen),
- einer fortlaufend dokumentierten und protokollierten Überprüfung der eingesetzten Software gegen die Prüfsummen,
- eine Betrachtung der Aspekte des Datenschutz, z. B. nach Maßgabe des “IT-Grundschutz” des Bundesamts für Sicherheit in der Informationstechnik (BSI).

Zur Veranschaulichung: Alle Bemühungen, ein beweissicheres Protokollierungssystem zu betreiben, werden unterlaufen, wenn nicht sichergestellt ist, dass kein Unbefugter Zugriff auf betriebskritische Komponenten bekommt. Dazu zählen neben der Hardware auch die Software des Betriebssystems (inklusive der ausgelieferten Bibliotheken), die sogenannten Router – die ja gerade den zu protokollierenden Netzwerkverkehr transportieren – und je nach Netzwerkkonfiguration weitere im selben Netzwerk betriebene Server.

Versionierung

Das Vorbringen von Stellungnahme 130319/04 (Anlage B 9) überrascht, da diese einzig die Unterschiede zwischen Versionen 1.47 und 1.50 des Systems “Observer” untersucht. Im vorliegenden Fall soll jedoch die Version 1.47 zum Einsatz gekommen sein, daher ist diese Anlage nicht von Belang.

In Gutachten 141117/04 (Anlage B 10) wird die begutachtete Version nicht benannt. Daher ist das Gutachten für die Bewertung der Beweissicherheit wertlos.

Auch Gutachten 140801/04 (Anlage B 11) stellt einzig die Versionsunterschiede zwischen 1.50 und 1.51 dar.

Stand der Technik

Aus Sicht des Gegengutachters entspricht die beschriebene Software nicht dem Stand der Technik. Wesentliche Leistungsmerkmale von Konkurrenzsystemen, die sich auf Nachvollziehbarkeit, Vermeidung von Irrtümern bei der Auskunft und die allgemeine Zuverlässigkeit des Systems auswirken, fehlen dem “Observer”.

1) Vergleichbare Systeme der Konkurrenz archivieren und signieren beispielsweise den gesamten auf der Netzwerkschnittstelle anfallenden Datenverkehr in einem der Standardformate für Netzwerkanalyse (z. B. PCAP). Dies erlaubt es, die vom System extrahierten Ergebnisse später unabhängig und mit frei verfügbaren Werkzeugen zu überprüfen oder mit neueren Versionen der selben Software zum Ausschluss von Fehlern zu wiederholen. Die dabei anfallenden Datenmengen können dabei inzwischen problemlos und kostengünstig auf handelsüblichen Archivmedien oder Festplatten gespeichert werden.

Wird hingegen wie beim “Observer” nur die Ausgabe des Software gespeichert und signiert, steht zu einer unabhängigen Nachprüfung der behaupteten Beobachtungen das Rohmaterial

nicht mehr zur Verfügung. Die Signatur bestätigt einzig und allein die – alle möglichen Fehler und Manipulationen beinhaltenden – Resultate der Auswertung.

Natürlich gibt es auch beim Ansatz eines Komplett-Archivs Möglichkeiten für Fehler und Manipulation, jedoch steigt der Aufwand für eine nachträgliche glaubwürdige Veränderung der Daten um ein Vielfaches.

2) Vergleichbare System der Konkurrenz stellen durch mehrfache Abfragen der Stammdaten sicher, dass Protokollierungsungenauigkeiten bei den Internetanbietern nicht zu Fehlauskünften führt.

Grob zusammengefasst hat ein Anbieter bei pauschaler Abrechnung (Flatrate) wenig Interesse an einer minutengenauen Protokollierung der Zuordnung vom Kunden zu seiner dynamisch zugewiesener IP-Adresse. Aus diesem Grund sind Auskünfte – anders als der Gutachter es in seinem **Zitat:**

“Daher ist es ausgeschlossen, dass zum Zeitpunkt der Aufzeichnung die aufgezeichnete IP-Adresse einem anderen Teilnehmeranschluss zugeordnet ist.”

darstellt – immer mit einem nicht zu vernachlässigenden Risiko der Fehlauskunft verbunden. Um sichere Fälle zu generieren, machen sich Konkurrenzsysteme die Eigenschaft des BitTorrent-Protokolls zunutze, dass Teilnehmer der Tauschbörse ein Interesse daran haben, auch nach Zwangstrennungen von den anderen Teilnehmern wiedererkannt zu werden. Dies ist in einem reputationsbasierten System wie BitTorrent wichtig, um trotz der sich durch die Trennung ändernden IP-Adresse die von anderen Teilnehmern gemessene “Größzügigkeit” beim Hochladen von Dateien attestiert zu bekommen, die in einigen privaten Filesharing-Gemeinden überhaupt erst die Teilnahme erlaubt.

Fällt nun derselbe Teilnehmer vor und nach der Zwangstrennung – also mit zwei verschiedenen IP-Adressen – unter der selben Kennung (in BitTorrent-Nomenklatur: peer_id) auf, und können die Stammdaten beider Abfragen auf den selben Anschluß zurückgeführt werden, kann ein doppelte Auskunftsfehler faktisch ausgeschlossen werden.

3) Vergleichbare System benutzen – wie alle modernen Softwareprojekte – für grundlegende Funktionalität aus Gründen der Zuverlässigkeit, Sicherheit und Wartbarkeit kostenlos sowie kommerziell verfügbare Programmbibliotheken. Ausweislich der aufgelisteten Namen der Quellcode-Dateien ist die beim “Observer” nicht der Fall.

Beispielhaft sind hier die Quellcode-Dateien “bdecoder.cpp” genannt. Die darin implementierten Funktionen werten mehrheitlich komplexe Datenstrukturen aus, die aus nicht vertrauenswürdigen Quellen stammen. Historisch gesehen sind Implementationsschwachstellen in solchen sogenannten “Parsern” häufige Fehlerquelle und das Einfallstor Nummer eins für Angriffe auf Softwaresystem.

Auch unnötig erneut implementierte Funktionalität, worauf die Dateinamen “crc32.c”, “linkstate .cpp” und “httpifc.c” in der Quellcodeliste des Gutachtens “120222/04” hinweisen, gehört nicht zu den “best practices”, also dem Konsens für Herangehensweisen an moderne Software. Es überrascht, daß der Dienstleister hier nicht auf Standard-Bibliotheken zurückgegriffen hat, bei denen jeweils eine Schar von freiwilligen Entwicklern über mehrere Jahre sicherheitstechnisch relevante und sonstige Implementierungsfehler bereinigt, die insbesondere auch auf die Verlässlichkeit der von der Software getroffenen Aussagen zurückfallen.

Die schlichte Auskunft des Gutachters:

Zitat:

“Der Sachverständige hat den zur Verfügung gestellten Quelltext untersucht und konnte sich von der einwandfreien Implementation überzeugen.“

wird dabei der Komplexität der dort neu-erfundenen Implementierungen der Protokolle nicht gerecht. Jede einzelne der Komponenten müsste strikten und wohldokumentierten Untersuchungen (Auditierungen) unterzogen werden, um als Bestandteil einer beweissicheren Installation infrage zu kommen.

Manipulationspunkte

Zitat:

“Für die Entstehung der Daten kann die forensische Integrität durch den Sachverständigen ohne Einschränkung bestätigt werden.”

Eine Bestätigung der “forensische[n] Integrität [...] ohne Einschränkung” ist eine unerfüllbare Zuschreibung an das System, wie ein einfaches Gedankenexperiment zeigt:

Bei (nicht eigens kryptographisch gesicherten) Netzwerkverbindungen kann die Identität der Gegenstelle außer durch die trivial zu fälschende Absenderkennung einzig dadurch etabliert werden, daß ein gesendetes Paket das Ziel erreicht. Zur Veranschaulichung: Wenn ich bei der Post einen Nachsendeauftrag für meine Adresse stelle, schickt die Post zur Überprüfung eine Postkarte an diese Adresse. Wenn ich die Karte empfangen und wieder bei der Post vorlegen kann, bin ich offensichtlich Inhaber der Adresse.

Aber genauso wie eine Postkarte auf dem Postweg abgefangen und betrügerisch vorgelegt werden kann, können Netzwerkpakete auf dem Weg automatisiert abgefangen, verändert oder künstlich erzeugt werden. Bei einer Karte können dies neben meinen Nachbarn mit Zugang zum Briefkasten auch Mitarbeiter der Post, inklusive aller Fahrer und Aushilfen. Im Internet können Nachbarn im Serverraum ebenso Pakete abfangen und fälschen, genauso wie alle Betreiber der Netzwerkinfrastruktur.

Die zitierte uneingeschränkte Bestätigung zeugt ganz offensichtlich von unsauberer Arbeit im Gutachten. Korrekt wäre gewesen, die Wahrscheinlichkeit und den verbundenen Aufwand für eine solche Manipulation darzulegen.

Im selben Gutachten relativiert der Gutachter sogar seine Aussage und stellt unbegründet ab:

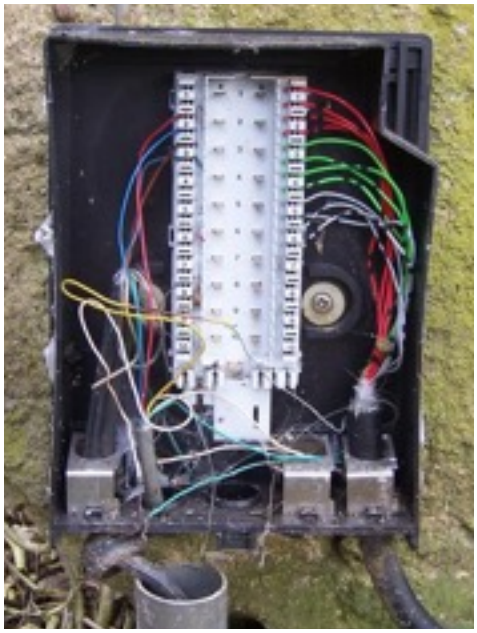
Zitat:

“(die theoretische Möglichkeit besteht, die praktische Ausführung ist jedoch höchst komplex und nicht einfach so durchführbar)”

Dem Autor dieses Gegengutachtens ist die genaue Umgebung unbekannt, in der das System “Observer” betrieben wird. Daher ist es schwer abzuschätzen, wie aufwändig genau die beschriebene Manipulation ist. Aus anderen Fällen sind dem Gegengutachters jedoch Szenarien bekannt, in dem das Protokollierungs-System aus Gründen der Tarnung an einer normalen Endkunden-DSL-Leitung betrieben wird.

Das Bedürfnis, sich zu tarnen, ist durch das Auftauchen öffentlicher Sperrlisten wie z. B. “Peer-Guardian” entstanden. In diesen Listen werden bekannte Netzwerkadressen von im Auftrag der Rechteinhaber agierenden Firmen veröffentlich. Dies erlaubt es Nutzern von Tauschbörsen, Verbindungen zu deren bekannt gewordenen Systemen zu vermeiden.

Der Betrieb eines Systems wie “Observer” auf einem angemieteten Rechner in einem gängigen Rechenzentrum ist daher unpraktisch, da diese Server zumeist nur eine oder wenige feste IP-Adressen zugeteilt bekommen, die nach Entdeckung quasi nutzlos sind. Zur Veranschaulichung: Genau wie im Telefonnetz anhand der Vorwahlen Anschlüsse geographisch zu verorten sind, können die ersten Stellen einer IP-Adresse Rückschlüsse zulassen, ob eine Gegenstelle bei der Telekom, Kabel Deutschland – oder eben in einem Rechenzentrum betrieben wird. Ganz paranoide File-Sharer blockieren daher jegliche Kommunikation zu IP-Adressen außerhalb von Endkunden-Netzbereichen.



DSL-Leitungen hingegen haben für Verfolger von Rechteverletzungen den natürlichen Vorteil, dass die Absenderkennungen (also IP-Adressen) ihrer Netzwerkverbindungen aus den zugeteilten Netzwerkbereichen stammen, aus denen sich auch der überwiegende Teil der anderen Tauschbörsen-Benutzer verbindet. Zudem werden vom Anbieter bei der Zwangstrennung regelmäßig neue IP-Adressen zugeteilt.

Wenn aber das “Observer”-System tatsächlich über die Kupferleitungen des DSL-Anbieters mit dem Internet verbunden ist, kann schon ein ungeschützter Telekom-Verteilerkasten im Hof eine bequeme und kostengünstige Angriffsstelle sein.

Vergleiche Sicherung der Leitungen im Verteilerkasten (Bild rechts, Quelle: http://up.picr.de/1926318.jpg) mit dem mehrstufigen Zugangssicherungskonzept in einem Rechenzentrum (Bild unten, Quelle https://blog.equinix.com/wp-content/uploads/2013/06/cage-540px.jpg).

Zitat:

“Der Sachverständige geht allerdings davon aus, dass die gültigen Sicherheitsregeln eingehalten werden.”

Wie auch im Abschnitt “Versionierung” angemerkt, ist eine vollständige Dokumentation über die Umgebung ist daher essentieller Bestandteil eines seriösen Gutachtens über die angebliche forensische Integrität.

Im Gutachten 120222/04 stellt der Gutachter fest:

Zitat:

“Es ist allerdings die Frage zu stellen, zu welchem Zweck eine solche Änderung vorgenommen werden sollte. Es wäre schon eine erhebliche kriminelle Energie notwendig, um die Daten so zu verändern, dass sie auf einen tatsächlich nicht Schuldigen zeigen.”

Tatsächlich ist zwar kriminelle Energie, aber bei einem Innentäter nicht viel technischer Aufwand vonnöten, Daten entsprechend zu verändern. Für ein technisches Gutachten ist diese Anmerkungen sehr tendenziös.

Um einen beliebigen Zweck einer solchen Änderung anzuführen: Gerade in einem sehr öffentlich verhandelten und potentiell teuren Fall hat zum Beispiel die Firma GuardaLey Ltd. selber ein starkes Interesse, einen eventuellen Protokollierungsfehler nachträglich zu korrigieren.

Ausschluss von Irrtümern

Alle im vorigen Abschnitt angeführten Punkte befassen sich mit böswilliger Manipulation, können sich jedoch leicht auf unabsichtliche Fehlerquellen übertragen lassen:

Während der Entwicklung von Software werden nach Stand der Technik große Mengen an Softwarekomponenten programmiert und auf das System angewendet, die korrekte Funktion im Normalbetrieb und angemessene Fehlerbehandlung bei unerwarteten Ereignissen testen sollen.

Ein Einfluß auf die Protokollierung von irrtümlich nicht korrekt abgeschalteten Testmodulen aus der Entwicklungsphase der Software müssen hierbei ebenso nachweislich ausgeschlossen werden, wie zum Testbetrieb vorgenommene und nicht rückgängig gemachte Änderungen an der Konfiguration der Systeme und ihrer Umgebung.

Korrektheit der festgestellten Tatsachen

In der Stellungnahme 120424/04 wird der Gutachter befragt:

Kann mit Hilfe des "Observers" sichergestellt werden. dass von den aufgezeichneten IP-Adressen jeweils eine vollständige Version einer urheberrechtlich geschützten Datei öffentlich zugänglich gemacht worden ist?

Seine Antwort:

Zusammen mit den vorstehenden Erläuterungen erscheint es nahezu ausgeschlossen, dass der vom "Observer" aufgezeichnete Client (bzw. dessen IP-Adresse) nicht die vollständige Datei zur Verfügung hat. Zwar kann nicht mit 100%iger Sicherheit ausgesagt werden, dass zum Zeitpunkt des ersten Mitschnitts die Datei in Gänze vorhanden ist, über den Zeitverlauf jedoch kann es als sicher gelten, dass die Datei vorliegen wird.

Im Gegensatz zu den Ausführungen des Gutachters ist ein Großteil der Versuche, eine Datei per BitTorrent herunterzuladen, nicht erfolgreich. Dies kann zahlreiche Gründe haben:

1) Oft ist keine vollständige Kopie des Dokuments mehr bei den Teilnehmern des Schwarms vorhanden, nachdem der ursprüngliche Anbieter (Seeder) ausgestiegen ist.
2) Oft werden auch bewußt von Urheberrechte-Inhabern beschädigte oder komplett inhaltsfremde Dateien unter dem Namen des eigenen Werks in Tauschbörsen gestellt, um Frustration bei den Filesharern zu erzeugen. Daher sind viele Teilnehmer dazu übergegangen, das selbe Werk mehrfach herunterzuladen.
3) Die Bandbreite einer üblichen Heimanbindung und die Kapazität von Festplatten ist begrenzt. Übliches Nutzungsmuster ist wie in 2) beschrieben, mehrere Versionen eines Werks im Hintergrund lange downloaden zu lassen. Wenn die Festplatte voll ist, oder die geschätzte verbleibende Rest-Download-Zeit kein realistisches Komplettieren eines Downloads erwarten lässt, werden die nur teilweise heruntergeladene Werke abgebrochen und dadurch die Fragmente gelöscht.

In allen Fällen hat der Teilnehmer schon aktiv seine heruntergeladenen “Pieces” wieder anderen angeboten, ohne je das komplette Werk auf seinem Rechner heruntergeladen zu haben.

Die Beantwortung dieser Frage entspricht offensichtlich nicht den Tatsachen.

Zusammenfassung

Zwar lässt das untersuchte Gutachten Rückschlüsse auf die Architektur des Systems “Observer” zu, jedoch lassen sich zur Qualität der Implementierung und Aussagekraft der Ergebnisse in Ermangelung des Quellcodes nur bedingt Aussagen treffen.

Wesentliche Komponenten des Gesamtsystems und die Betriebsumgebung sind zudem nicht Bestandteil des Gutachtens. Rückschlüsse auf die Beweissicherheit der protokollierten IP-Adressen lässt das Gutachten daher nur schwerlich zu. Von einer lückenlosen Beweisführung ist sicherlich nicht zu sprechen.

Die Beschreibung von Architektur und Struktur der Software deuten stark darauf hin, dass das System “Observer” nicht dem Stand der Technik entspricht. Wichtige Leistungsmerkmale zur Garantie von Zuverlässigkeit der Software und deren Protokollierung fehlen.

Eine kritische Betrachtung der begutachteten Software ist im Gutachten selber nicht dokumentiert. Typische Anzeichen einer fachgemäß ausgeführten Auditierung fehlen, streckenweise wirkt das Gutachten eher wie eine Software-Dokumentation.

Teile der im Gutachten gemachten Aussagen entsprechen zudem nicht den Tatsachen.