Die dunkle Seite von I2P, einer Fallstudie zur forensischen Analyse

Behnam Bazli, Maxim Wilson & William Hurst

Published online: 12 Jun 2017.
To cite this article:
Behnam Bazli, Maxim Wilson & William Hurst (2017) The dark side of I2P, a forensic analysis case study, Systems Science & Control Engineering, 5:1, 278-286, DOI: 10.1080/21642583.2017.1331770
To link to this article:
https://doi.org/10.1080/21642583.2017.1331770

ABSTRAKT

Filesharing-Anwendungen, die als Peer-to-Peer-Netzwerk (P2P) fungieren, sind aufgrund ihrer Heterogenität, ihres dezentralen Ansatzes und ihrer rudimentären Bereitstellungsfunktionen bei Benutzern und Entwicklern beliebt. Sie werden jedoch auch für illegale Online-Aktivitäten verwendet und sind häufig von böswilligen Inhalten wie Viren und Schmuggelware befallen. Dies bringt neue Herausforderungen für forensische Untersuchungen beim Erkennen, Abrufen und Untersuchen der P2P-Anwendungen mit sich. Innerhalb der Domäne von P2P-Anwendungen wird das Invisible Internet Project (IP2) verwendet, um Anwendungen die Kommunikation mit einem Namen zu ermöglichen. In dieser Arbeit wird die Verwendung durch Netzknotenbetreiber und bekannte Angriffe auf die Privatsphäre oder Verfügbarkeit von I2P-Routern erörtert. Insbesondere untersuchen wir die Eigenschaften von I2P-Netzwerken, um die Sicherheitsmängel und die Probleme beim Erkennen von Artefakten im I2P zu skizzieren. Darüber hinaus diskutieren wir neue Methoden zum Erkennen des Vorhandenseins von I2P mithilfe von Forensictools und zum Rekonstruieren spezifischer I2P-Aktivitäten mithilfe der verbleibenden Artefakte über die Netzwerksoftware.

1. Einführung

Selbstorganisierende Overlay-Netzwerke, die auf IP-Netzwerke verteilt sind, werden als P2P-Netzwerke bezeichnet. Sie sind skalierbare Plattformen und für den Dateiaustausch beliebt, da eine Reihe von Plattformen für die Inhaltsverteilung verfügbar sind (Valdez, Guirguis, Wingate & Rinkevich, 2011). 2P-Filesharing-Netzwerke spiegeln das Paradigma des Internet der Dinge (IoT) wider, mit autonomen vernetzten Geräten in verteilten und dezentralen Systemen. Die Topologie von P2P-Netzwerken ist gegenüber einem herkömmlichen Client-Server-Ansatz von Vorteil, da sie selbst skalierbar sind (Braun, Ekler & Fitzek, 2016) und die Menge der verfügbaren Daten proportional zur Anzahl der Teilnehmer ist. Im Allgemeinen werden P2P-Netzwerke von Protokollen verwaltet, die auf Anwendungsebene über dem User Datagram Protocol (UDP) oder dem Transmission Control Protocol (TCP) implementiert sind. Darüber hinaus unterstützen P2Poverlays die Skalierbarkeit in dynamischen und dezentralen Systemen. Die Knoten innerhalb eines P2P-Systems verhalten sich im Gegensatz zum Client-Server-Modell selbstverwaltend. Solche Overlay-Netzwerke gehen über die Dienste hinaus, die herkömmliche Client-Server-Systeme anbieten (Wei, Wang, Chu & Chang, 2012). P2P-Systeme sind weit verbreitet und werden hauptsächlich für den Dateiaustausch und die Datenkommunikation verwendet.

Während das schnelle Wachstum und die allgegenwärtige Nutzung von File-Sharing-Anwendungen für die Benutzer im Allgemeinen positiv ist, ergeben sich für forensische Untersuchungen zahlreiche Herausforderungen: Zumal das IoT weitere intelligente Geräte einführt, die zum Volumen des Netzwerkverkehrs beitragen (Braun et al ., 2016). Dies wird durch die ständigen dynamischen Änderungen der Mitgliederzahlen, die geopolitische Haltung in Bezug auf urheberrechtliches Material und die rechtlichen und ethischen Aspekte, die sich aus dem Umgang mit Filesharing-Anwendungen ergeben, noch verschärft. Das größte Problem ist jedoch die Überwindung der durch die Funktionen des P2P-Netzwerks hervorgerufenen Missbräuche, insbesondere innerhalb der I2P-Umgebung. Viele Strafverfolgungsbehörden bemühen sich, mit den neuen Tools und Techniken Schritt zu halten, die von P2P / I2P-Nutzern, die zu Online-Aktivitäten beitragen und diese ermöglichen, missbraucht werden. Aus diesem Grund untersuchen wir die Eigenschaften von I2P-Netzwerken und verwandten Anwendungen, die für Aktivitäten attraktiv und problematisch sind für den forensischen ana-lyst. Darüber hinaus schlagen wir alternative Ansätze vor, um die Aktivität eines Verdächtigen in einem I2P-Netzwerk zu identifizieren und zu rekonstruieren und die verbleibenden Artefakte zu analysieren. Um dies zu erreichen, wird eine Kombination aus kundenspezifischen und branchenerprobten spezifischen Werkzeugen eingesetzt. Dieses Dokument ist wie folgt aufgebaut. Abschnitt 2 stellt das I2P-Netzwerk, seine aktuellen Entwicklungen und die Herausforderungen vor, die es bei forensischen Untersuchungen darstellt. Abschnitt 3 beschreibt das Lösungsdesign und die Beschreibung der forensischen Verfahren in I2P-Untersuchungen. Abschnitt 4 enthält verwandte Arbeiten und Abschnitt 5 enthält eine Diskussion und eine zukünftige Ausrichtung der Forschung.

1.1. Netzwerk-Overlay

Das Netzwerk-Overlay unterstützt die Skalierbarkeit in einem dynamischen und dezentralen System mit selbstverwaltenden Knoten (Nadeem & Karamat, 2016). Dies bedeutet, dass sie die verfügbaren Ressourcen, Inhalte und die Stabilität des Datenverkehrs unabhängig von zentralen Servern nutzen können. Nodeshave verfügt über zwei Client- und Serverrollen und kann eingehende Verbindungen initiieren und überwachen.

Overlay-Netzwerke arbeiten über einem anderen Netzwerk (als „Basis“ bezeichnet) und bieten zusätzliche Funktionen, die das Basisnetzwerk nicht bietet. Da Overlay-Netzwerke die direkte Interaktion mit zugrunde liegender Hardware vermeiden, können sie für interessierte Benutzer bereitgestellt werden, ohne dass ein kostspieliges Upgrade der Infrastruktur oder eine Unterbrechung der Basisnetzwerkdienste erforderlich ist.

Gegenwärtig gibt es drei ausgereifte Overlay-Netzwerke, die das Internet als Basis nutzen und es durch Hinzufügen von Datenschutzfunktionen verbessern. Tor, Freenet und I2P. Diese Netzwerke sind Open Source und wurden vor mehr als 10 Jahren für die Öffentlichkeit freigegeben und befinden sich noch in der aktiven Entwicklung. Diese Arbeit konzentriert sich jedoch auf die Untersuchung des I2P-Netzwerks aufgrund seines Potentials für zukünftiges Wachstum und der öffentlichen Wahrnehmung, dass es die sicherste der drei Lösungen ist.

1.2. P2P-Netzwerke

Ein Netzwerk-Overlay ist eine Lösung für die Skalierbarkeitsprobleme in verteilten Systemen (Jayashree & Peru-mal, 2014). Es ist ein virtuelles Netzwerk von Knoten und Logikverbindungen, das auf der vorhandenen Netzwerkinfrastruktur aufbaut. Es kann daher verwendet werden, um zusätzliche Dienste und Funktionen bereitzustellen, die vom Basisnetzwerk nicht angeboten werden. Da das Netzwerk keine direkte Interaktion mit der zugrunde liegenden Infrastruktur aufweist, kann es bereitgestellt werden - keine kostspieligen Upgrades oder Unterbrechungen der Basisnetzwerkdienste. Darüber hinaus ist keine Änderung vorhandener Software oder Protokolle erforderlich, damit neue Knoten dem Overlay-Netzwerk beitreten können.

Ein P2P-Overlay unterstützt die Skalierbarkeit in einem dynamischen und dezentralen System mit selbstverwaltenden Knoten. Dies bedeutet, dass alle Knoten zum gemeinsam genutzten Pool von Netzwerkressourcen und -inhalten beitragen und davon profitieren, ohne auf einen zentralen Server angewiesen zu sein. P2P-Netzwerke mit verschiedenen Eigenschaften, die auf der Grundlage verschiedener Methoden wie Leistungsmetriken, Topologie, Protokoll und Struktur klassifiziert wurden (Jawad, Serrano-alvarado & Val-duriez, 2013). P2P-Overlays sind bei Benutzern für Dateifreigabe und Kommunikation wie

Skype, 1Bit-Torrent2 und Freenet.3 beliebt. Jede Klasse des Systems hat ihre eigenen Vor- und Nachteile, der Schwerpunkt liegt jedoch auf P2P-Overlays, die ihren Benutzern ein gewisses Maß an Anonymität bieten. Anonymität ist das Hauptmerkmal, das die Privatsphäre des Benutzers gewährleistet. Diese Funktion ist für unerlaubte Handlungen vorgesehen, die auf dem Teilen von urheberrechtlich geschütztem Material, illegalen Transaktionen und allgemeinen Internetkriminalitäten beruhen.

1.3. I2P-Netzwerk

Das I2P ist eine Adaption von Kademlia (Clarke, 1999), die ursprünglich entwickelt wurde, um einen Schritt weiter zu gehen als nur Anonymität. Benutzer können sich in unsichtbaren Räumen befinden, die als „Darknet“ bezeichnet werden. I2P bietet einen P2P-Kommunikationskanal sowie verschiedene Protokolle und Verschlüsselungsstandards, um die Anonymität der Benutzer zu gewährleisten. Die End-to-End-Kommunikation zwischen zwei Benutzern wird nicht global beworben. Darüber hinaus ist es vollständig verschlüsselt. I2P verbessert das standardmäßige TCP / IP-Kommunikationsmodell, indem sichergestellt wird, dass IP-Pakete (Internet Protocol), die zwischen teilnehmenden Hosts ausgetauscht werden, immer verschlüsselte Daten enthalten. Anstatt sich auf IP-Adressen zu verlassen, um Hosts und Routing-Traffics eindeutig zu identifizieren, führt I2P seine eigenen Bezeichner und Routing-Logik auf einer höheren Ebene des Protokollstapels ein. Solange eine Layer 4-Netzwerkkonnektivität zwischen Hosts besteht, ist I2P in der Lage, sich vollständig von der öffentlichen Internetinfrastruktur zu trennen. Diese Verbesserungen zielen darauf ab, die Anonymität der Benutzer zu verbessern, indem das Risiko von böswilligen Dritten wie einem kompromittierten Dienstanbieter verringert wird und der Netzwerkverkehr abgefangen oder geändert wird. Diese Sicherheits- und Datenschutzverbesserungen werden insbesondere von I2P-Benutzern in Ländern mit restriktiven Richtlinien geschätzt Regelung der Internetnutzung. Dieselben Funktionen können jedoch ein Problem für Strafverfolgungsbehörden darstellen, sodass I2P eine attraktive Lösung für Cyberkriminelle darstellt, um ihr Geschäft sicher zu betreiben. In diesem Abschnitt werden die Merkmale der I2P-Anwendungen erläutert.

1.3.1. I2P-Router

I2P-Knoten kommunizieren über einen P2P-Tunnel, der von I2P-Routern unterstützt wird. Die I2P-Knoten und -Router kommunizieren über eine Tunnelinfrastruktur vom Typ Knoblauchzehen. Die durchgängige Kommunikation verwendet eine Form von Public KeyInfrastructure (PKI). Die eingehenden Tunnel sind jedoch von den ausgehenden Tunneln getrennt. Der Absender hat keine Informationen oder Kenntnisse über die ausgehenden Routen. Vorausgesetzt, die übertragenen Nachrichten werden mithilfe des I2Prouter viele Male weitergeleitet, wodurch die Benutzeridentität vollständig

ausgeblendet wird. Die Kommunikation zwischen Peers hat keinen Ein- oder Ausgangspunkt. Dies verhindert, dass in ähnlichen Systemen wie Tor (McCoy, Bauer, Grunwald, Kohno, & Sicker, 2008) eine Sicherheitslücke besteht).

1.3.2. I2PSnark

I2PSnark ist der Standard-Torrent-Client für das I2P-Netzwerk und wird als Teil der I2P-Routersoftware (Timpanaro, Chrisment & Festor, 2012) vertrieben. Als native I2P-Anwendung verarbeitet I2PSnark keine Standard-IP-Adressen und ist daher nicht in der Lage, überdurchschnittliches Internet zu kommunizieren. Diese Einschränkung ist beabsichtigt und stellt sicher, dass kein persönlich identifizierter P2P-Verkehr außerhalb des verschlüsselten I2P-Tunnels lecken kann. Sicherheit und Benutzerfreundlichkeit gewährleisten die anhaltende Beliebtheit von I2PSnark bei I2P-Netzwerkbenutzern. Die I2PSnark-Benutzerbasis ist größer als die aller anderen I2P-Kunden zusammen, wobei I2PSnark für ein Drittel des gesamten I2P-Netzwerkverkehrs verantwortlich ist.

P2P (BitTorrent) -Clients, die über das normale Internet betrieben werden, versorgen jedes Mitglied des Torrent-Schwarms mit Informationen über alle anderen Peers. Ein forensischer Prüfer kann daher den Speicherort und die IP-Adresse des Erstellers des Torrents abrufen, die dann von Gerichten und dem Internetdienstanbieter überprüft werden, um die Identität des Dateifreigabemoduls zu bestimmen. Wenn Sie diese Methode auf I2PSnark anwenden, erhalten Sie lediglich eine Liste der I2P-Netzwerkkennungen von Peers, die keinen forensischen Wert haben.

1.3.3. Domainnamensauflösung

I2P ist fehlertolerant und widersteht unbeabsichtigten oder absichtlichen Ausfällen öffentlicher Internetdienste. Ein Beispiel für einen solchen öffentlichen Dienst ist das Domain Name System (DNS), das für die Übersetzung von Benutzernamen mit Leserechten in die entsprechenden IP-Adressen zuständig ist. Die öffentliche DNS-Infrastruktur des Internets ist streng hierarchisch aufgebaut. Domänen der obersten Ebene (z. B. ".com") werden von einer neutralen, nichtkommerziellen Organisation, der Internet Corporation for Assigned Names and Numbers (ICANN), verwaltet. Domänen niedrigerer Ebene (z. B. ". Co.uk") werden von Hosting-Unternehmen, kleineren Unternehmensverbänden oder Einzelpersonen kontrolliert. Die Hierarchie ist in Abbildung 1 wie folgt dargestellt.

Ein mit dem Internet verbundener Host kann diese Domänennamen auflösen, indem iterative Abfragen an jeden DNS-Server in der hierarchischen Kette gesendet werden. Diese Methode stellt sicher, dass die endgültige Antwort authentisch, genau und aktuell ist. Sie ist jedoch ineffizient und lässt sich nur schlecht auf mehrere Hosts skalieren. Die Lösung wird verzögert, indem auf Antworten von mehreren Servern gewartet wird. Darüber hinaus führen mehrere Hosts, die denselben Domänennamen abfragen, die gleiche Aufgabe wiederholt aus. Ein üblicher alternativer Ansatz besteht darin, diese Aufgabe

auf einen einzelnen DNS-Server zu verlagern, auf dem vom Host angeforderte Abfragen durchgeführt werden. Dieses Setup ist sowohl in Heim- als auch in Unternehmensumgebungen üblich, in denen interne Hosts alle ihre Abfragen an den DNS-Cache-Server senden, der von ihrem Internet-Service-Provider oder von ihrem Unternehmen verwaltet wird.

Die öffentliche DNS-Infrastruktur basiert daher auf Vertrauen, wobei jeder Host davon ausgeht, dass die Server in höheren Ebenen weiterhin genaue Daten bereitstellen. Die hierarchische Struktur kann sowohl zu technischen Ausfällen als auch zur Übernahme von Domain-Namen durch böswillige Dritte führen. Eine solche Infrastruktur eignet sich nicht für I2P, bei der Zuverlässigkeit und Anonymität der Benutzer im Vordergrund stehen. Aus diesen Gründen implementiert das I2P-Netzwerk ein eigenes System zum Auflösen kurzer, von Menschen lesbarer Domänennamen.

Als Teil des entwickelten Systems muss jeder Knoten in einem I2P-Netzwerk ein lokales Adressbuch führen. Das Adressbuch ist eine Datei, in der die Verknüpfungen zwischen einem I2P-Domänennamen und einer I2P-Netzwerkkennung (als Ersatz für die IP-Adresse) gespeichert werden. Das Konzept ähnelt der Verwendung von Host-Dateiknoten des frühen Internets vor der Einführung von DNS (Hesselman, Moura, de OliveiraSchmidt & Toet, 2017).

Um die Notwendigkeit der manuellen Bearbeitung von Host-Dateien zu verringern, implementiert I2P einen Mechanismus, der als "Abonnements" bekannt ist. Ein I2P-Knoten kann mehrere andere Knoten im I2P-Netzwerk als Abonnementquellen angeben, die regelmäßig nach ihren Kopien des Adressbuchs abgefragt werden. Alle Einträge der Domänennamen, die nicht im Adressbuch des abonnierten Knotens vorhanden sind, werden mit der aktuellen Kopie zusammengeführt.

Das Ziel des beschriebenen I2P-Systems ist es, so viele Informationen wie möglich zu behalten, um Domainnamen lokal auf dem I2P-Knoten aufzulösen. Daher ist es unwahrscheinlich, dass ein forensischer Analytiker, der Namensauflösungs-Abfrageprotokolle vom Internetdienstanbieter des I2P-Benutzers, vom lokalen DNS-Caching-Server oder vom DNS-Resolver-Cache abruft, Einträge im Zusammenhang mit dem I2P findet.

1.3.4. Darknets

I2P verwendet einen eigenen Domain-Namen-Service, der die Existenz von "Eepsites" ermöglicht, die auch als "Darknets" bezeichnet werden. Sie gelten als versteckte Websites, auf die nur Benutzer zugreifen können, die mit dem I2P-Overlay-Netzwerk verbunden sind (Coudriau, Lahmadi, & Francois, 2016). Eepsites werden direkt auf I2P-Netzwerkknoten gehostet und über Domainnamen abgerufen, die an die Top-Level-Domain ".i2p" gesendet werden (siehe Abbildung 2).

Bei einer Untersuchung einer normalen Internet-Website können die Domain-Registrierungsdatensätze und die Kopie der DNS-Zonendateien mehrere

Schlüsselelemente und forensisch wertvolle Informationen enthalten. Dazu gehören die Kontaktdaten des Domaininhabers, die persönlichen Daten des Domaininhabers und die Mailexchange-Aufzeichnungen, die die IP-Adresse des Hosts angeben. Auf diese Weise kann die Identität des Website-Inhabers identifiziert, die betroffene Domain eingerichtet und der Webhost-Server für weitere Zwecke beschlagnahmt werden Untersuchung durch den forensicanalyst.

Ein solcher Ansatz ist gegen I2P-Eep-Stellen nicht wirksam. Normale Internet-Registrare sind Teil der DNS-Hierarchie und werden daher aufgefordert, mit den Strafverfolgungsbehörden des ICANN-4-Schemas (Internet Corporation for AssignedNames and Numbers) zusammenzuarbeiten. Durch die Registrierung eines Domainnamens auf einer Website wird sichergestellt, dass keine persönlichen Informationen oder IP-Adressen von der Registrierungsstelle gespeichert werden. Die Registrierungsstellen für I2P-Domainnamen sind anonym. Sie haben kein Leitungsgremium und sehen sich keinen Konsequenzen gegenüber, wenn sie Regeln, Vorschriften und Anfragen von Strafverfolgungsbehörden ignorieren.

Der Zugriff auf verborgene Seiten ist für Suchmaschinen wie den Google-Suchcache und Wayback-Maschinen nicht sichtbar. Forensische Analysten stützen sich häufig darauf, um den Inhalt der verdächtigen Website zu einem bestimmten Zeitpunkt nachzuweisen. Eepsites sind daher weniger konsistent als normale Websites, da keine Sicherungskopie gespeichert ist, die gefunden werden kann, wenn sie vom Eigentümer heruntergefahren wird.

1.3.5. Erkennen einer I2P-Installation

Die möglichen Missbräuche des I2P-Netzwerks sind Strafverfolgungsbehörden und forensischen Analysten weniger bekannt. Dies kann dazu führen, dass die I2P-Installation auf einem beschlagnahmten Computer nicht entdeckt und als Quelle potenziell wertvoller forensischer Artefakte identifiziert wird. Die in der Industrie zugelassene Software wie EnCase, Autopsy und FTK verfügt über keine Analyse- oder Erkennungsfunktionen für I2P-Artefakte. Als solche geben sie keinen Hinweis auf das Vorhandensein von I2P-Artefakten. Außerdem kann die Aktivität des I2P auf dem zu untersuchenden System in einem der beiden Modi auf einer Windows-Maschine installiert werden. entweder als anwendung oder als systemdienst. Die Systemdienstinstallationen von I2P sind für forensische Analysten von größerem Wert. Dies liegt daran, dass Benutzer, die für das Hosten von Epsites eine permanente Verbindung zu I2P benötigen oder illegale Inhalte freigeben, den I2P-Installationsdienst bevorzugen. Als Systemdienst installiertes I2P ist jedoch aufgrund fehlender Einträge in der StartMenu, Desktop und Most Recently Used (MRU) -Softwareliste eine größere Herausforderung.

2. Forensische Analyse von I2P

Um die Diskussion in diesem Abschnitt fortzusetzen, stellen wir verschiedene Methoden zur forensischen Untersuchung von I2Partefakten vor. Wir nutzen die Merkmale und Schwachstellen von I2Pactivities, um eine umfassende und effektive Methode vorzuschlagen, die im Rahmen forensischer Untersuchungen eingesetzt werden kann. Solche Techniken sind in bestehende Tools integriert, um Untersuchungen effizienter zu gestalten.

Die I2P-Routersoftware konzentriert sich stark auf die Sicherheit des Netzwerkverkehrs und nicht auf die lokal auf den beteiligten I2P-Knoten gespeicherten Daten. Infolgedessen werden die lokalen Daten unverschlüsselt gespeichert und können zur forensischen Analyse einer beschlagnahmten Maschine verwendet werden. Darüber hinaus zeigen wir auf, wie die Funktionen und Mängel innerhalb des Netzwerks bei forensischen Untersuchungen berücksichtigt werden sollten.

2.1. Untersuchung von I2P-Installern

I2P-Installationsprogramme für die Windows-Betriebssystemfamilie enthalten mehrere Ebenen. Die äußere Ebene ist ein selbstextrahierendes Archiv im 7-Zip-Format, mit dem die Installationskomponenten in einer einzelnen Datei verteilt und die Dateigröße verringert werden. Die innere Ebene ist eine PACK-Datei, die vom IzPack-Installationsprogramm für in Java geschriebene Anwendungen erstellt wird. Obwohl für die von IzPack generierten Dateien kein offizieller Entpacker vorhanden ist, ähnelt die Struktur der Paketdatei leicht der eines forensischen Images und kann daher umgekehrt werden. Die IzPack-Paketdatei enthält einen allgemeinen Dateikopf, gefolgt von Dateien, die zu einzelnen Komponenten der I2P-Routersoftware gehören. Einzelne Komponentendateien innerhalb des Pakets werden durch Kopf- und Fußzeilensignaturen gekennzeichnet, in denen auch der Name der Komponentendatei, der Typ und der Pfad für die beabsichtigte Installation aufgeführt sind.

Diese Komponentendateien können mit einem einzigen Skript extrahiert werden, das in einer Programmiersprache wie Python geschrieben ist, das mit den meisten forensischen Tools kompatibel ist, und anschließend entweder zum Erstellen einer Hash-Set-Bibliothek oder zum manuellen Vergleich durch den forensischen Analysten verwendet werden.

2.2. Erkennung über bekannte Hash-Set-Bibliothek

Aus den einzelnen I2P-Komponenten, die aus den Installationsdateien extrahiert wurden, können Hash-Set-Bibliotheken erstellt werden. Diese Bibliotheken können in genehmigte forensische Software importiert werden, die das Vorhandensein derzeit nicht erkennen kann, wenn I2P keine Beweise enthält. Die EnCase Suite von Guidance Software ist ein Beispiel für ein forensisches Tool, das für die Erstellung von rechtsgültigen forensischen

Berichten zugelassen ist, I2P in seiner Standardkonfiguration jedoch nicht erkennen kann. EnCase unterstützt jedoch die Verwendung von Hash-Bibliotheken, die MD5 und SHA1 enthalten.

EnCase kann daher für die Erkennung von I2P ausgestattet werden, indem eine alte Hash-Bibliothek importiert wird, die MD5-Hashes von I2P-Komponenten enthält. Einige Komponenten von I2P sind für diese Erkennung besser geeignet als andere aufgrund ihrer sich ändernden Attribute. Zum Beispiel ist die I2P-Anwendung selbst kein guter Kandidat für eine Hash-Bibliothek, da sich die Hashes mit der häufigen Veröffentlichung von I2P ändern. Die digitalen Zertifikate von I2P developer eepsite sind jedoch gute Kandidaten, da sie in jeder I2P-Knoteninstallation vorhanden sind und über mehrere Versionsversionen hinweg nicht betroffen sind.

2.3. Vergleich von Adressbüchern

Eine der Komponenten des I2P, die aus dem I2P-Installationsprogramm extrahiert werden kann, ist die Kopie des Standardadressbuchs. Jeder neue I2P-Knoten wird während der Installation mit der gleichen Kopie dieses Adressbuchs ausgestattet, sodass er auf ein Minimum an vertrauenswürdigen Eepsites zugreifen kann. Der I2P-Knoten sollte dann dieses minimale Adressbuch erweitern, indem er Informationen aus seinem eigenen Satz von Abonnementquellen importiert und Domainnameneinträge für die E-Site manuell hinzufügt.

Der forensische Analyst kann dieses minimale Standardadressbuch als Referenz verwenden, um es mit dem Adressbuch zu vergleichen, das auf dem beschlagnahmten Computer gefunden wurde. Einträge, die nicht im Standardadressbuch gefunden wurden, wurden entweder über Abonnementaktualisierungen importiert oder manuell vom I2P-Knotenbesitzer hinzugefügt. Eepsite-Einträge, die aus einem Abonnement stammen, können durch Einsehen des Subskriptions-Aktualisierungsprotokolls, wie z. B. Uhrzeit, Quelle und Domänenname des importierten Eintrags, weiter aus dieser Liste entfernt werden. Durch diesen Eliminierungsprozess kann das Adressbuch von einem beschlagnahmten Computer auf einen Satz von Domäneneinträgen reduziert werden, die höchstwahrscheinlich vom Besitzer des I2P-Knotens manuell für sein persönliches Surfen auf der E-Site hinzugefügt wurden. Diese Informationen können besonders nützlich sein, wenn der Verdächtige kriminalpolizeiliche Maßnahmen ergriffen hat, um Browserverlauf und Artefakte von seinem lokalen Computer zu entfernen.

2.4. Übernahme bestehender Registrare

Registrare im I2P-Netzwerk müssen kein Akkreditierungs- oder Genehmigungsverfahren durchlaufen. Dies ermöglicht es jedem Interessenten, seinen eigenen I2P-Domainnamen-Registrar-Knoten zu betreiben. Obwohl es für Strafverfolgungsbehörden oder forensische Analysten möglich ist, ihre eigenen

neuen Registrare im I2P-Netzwerk einzustellen, können einige der bekannten guten Registrare bei der Übernahme verwundbar werden. Der Hauptkandidat für die Übernahme wäre Beregistrar mit der Bezeichnung „NO.i2p“. NO ist ein kleiner Registrar im Vergleich zu Entwicklern wie "Stats.i2p", nimmt jedoch eine Sonderstellung im I2P-System zur Namensauflösung ein.

NO teilt nicht die von "Rogue" -Registrierern wie INR betriebene Freigaberichtlinie. Stattdessen teilt NO die gleiche Version der Registrierungsrichtlinie mit Entwicklern, die illegale oder fragwürdige Inhalte verbietet. Da es keine politischen Meinungsverschiedenheiten gibt, ist NO einer der wenigen Registrars, die vom I2P-Projektteam als "vertrauenswürdig" eingestuft werden. Als vertrauenswürdiger Registrar ist dies eine von nur vier Dienstoptionen, die jedem I2P-Benutzer angezeigt werden, der versucht, auf eine Website zuzugreifen, die dem lokalen Adressbuch nicht bekannt ist.

Ab Anfang 2016 scheint der NO-Registrar von seinem Besitzer verlassen worden zu sein. Neue Domain-Anfragen können weiterhin von Nutzern über die Website von NO eingereicht werden, werden jedoch vom Betreiber nicht geprüft. Die Datenbank der vorhandenen Domains wurde nicht gesäubert oder auf Verstöße gegen den Inhalt überprüft, da NO weiterhin Namenseinträge für Ressourcen speichert, die gegen seine eigenen Registrierungsbedingungen verstoßen, z. B. die I2Pmirror of Silk Road Reloaded-Website.

Die mangelnde Wartung zusammen mit dem Status "vertrauenswürdig" sollte NO zu einem attraktiven Ziel für die Strafverfolgung und böswillige Parteien machen. Aufgrund mangelnder Wartung erhält NO derzeit keine Sicherheitsupdates für seine I2P-Routersoftware oder den Webserver. Ein Angriff mit der Fähigkeit, Kompromisse einzugehen, kann die Kontrolle über einen wichtigen Teil der I2P-Infrastruktur erlangen.

Die alternative Möglichkeit wäre, bis zum Ausfall von NO oder seines I2P-Servers zu warten und auf Social Engineering zurückzugreifen. Bei den meisten I2P-Registraren, einschließlich NO, handelt es sich um eine Software zur Namensauflösung, die als Py-I2PHosts bekannt ist und über die Entwicklerseite im I2P-Netzwerk heruntergeladen werden kann. Es ist daher möglich, NO afterits Fehler auf verschiedenen B32- und eepsite-Adressen neu zu erstellen. Der neu erstellte Registrar kann dann auf den I2Pcommunity-Ressourcen angekündigt werden, nachdem ein Hardwarefehler aufgetreten ist.

Ein Erfolg dieser Methode ist aufgrund der dezentralen Struktur der I2P-Benutzer möglich, bei denen keine Kontrolle über die Mitgliedschaft besteht. Jeder Benutzer kann einen hochwertigen Netzwerkdienst ohne Ressourcen einrichten. Der Registrar „RUS.i2p“ war dafür bekannt, dass er I2P-Knowledgebase- und -Peepsite-Einträge für Benutzer in Ländern außerhalb der GUS-Staaten hostete. Nach mehreren längeren Ausfällen und Wiederherstellungen von Diensten ist dieser Registrar einem Server-Hardwareausfall erlegen und nicht mehr verfügbar. Ein anderer I2P-Registrar, "NIC.i2p", ist nicht mehr an seinem ursprünglichen Eepsite-Domainnamen

beteiligt und kann nur über seine vollständige Netzwerkadresse erreicht werden. Mehrere I2P-Betreiber empfanden diesen Vorfall als verdächtig und stellten die Fähigkeit des Betreibers in Frage, einen kritischen Netzwerkdienst auszuführen. Trotzdem bleibt der Registrar zum Zeitpunkt dieses Berichts in Betrieb und ist in nicht offiziellen, bekannten Registrar-Listen enthalten, die in der I2P-Benutzergemeinschaft verbreitet werden.

2.5. Spiegelung von Eepsites

Das nicht hierarchische Modell des I2P-Namensauflösungssystems ermöglicht es dem forensischen Analysten, einen eigenen Spiegel der verdächtigen Website zu erstellen und unter demselben Domainnamen zu registrieren. Domain-Namen in I2P sind nur als Uniqueper-Registrare registriert und können gleichzeitig bei mehr als einem Host registriert werden (siehe Abbildung 2).

Aufgrund der komplexen Verbreitung von I2P-Namensaktualisierungen ist es möglich, dass der vorhandene Domainname auf verschiedenen Registraren verfügbar bleibt. Beispielsweise werden über I2P registrierte Domain-Namen, die als INR bezeichnet werden, aufgrund des nicht vertrauenswürdigen Status von INR nicht immer an andere Registrare weitergegeben.

Diese Methode der Penetration sollte auch in Bezug auf eine Besonderheit des I2P-Benennungssystems in Betracht gezogen werden: die Persistenz von Namensdatensätzen. Sobald das Adressbuch des I2P-Knotens gespeichert ist, läuft es niemals ab. Der Registrar, von dem diese Informationen stammen, hat möglicherweise die Informationen ursprünglich aktualisiert oder die Domain vollständig aus seiner Datenbank gelöscht. Keines dieser Ereignisse wirkt sich jedoch auf einen vorhandenen Adressbucheintrag aus. Der Eigentümer, das Personal und die regelmäßigen Besucher der gespiegelten I2P-Site werden dadurch nicht von der auf der falschen Spiegel-Site durchgeführten Informationsbeschaffung betroffen sein.

Die dauerhaften Adressbucheinträge wirken sich zugunsten eines forensischen Analytikers oder einer Strafverfolgungsbehörde aus. Eepsite-Besitzer und regelmäßige Besucher sind mit größerer Wahrscheinlichkeit sicherheitsbewusst und mit dem "Look and Feel" der gefährdeten Eepsite bestens vertraut. Dieses Wissen erhöht die Gefahr, dass einer der Besucher Inkonsistenzen auf der Site des falschen Spiegels entdeckt und andere Benutzer alarmiert. Im Vergleich dazu ist die Wahrscheinlichkeit, dass neue oder gelegentliche Besucher alarmiert werden, geringer, da sie keine Referenz haben, mit der sie die Mirroreepsite vergleichen können.

Der sich daraus ergebende Vorteil ist, dass eepsite mit falschem Spiegel über einen langen Zeitraum unentdeckt bleiben kann und ständig Informationen über die Aktivität neuer Besucher sammelt. Je länger die falsche Eepsite in Betrieb bleibt, desto höher ist die Wahrscheinlichkeit, dass sie einen der regelmäßigen Besucher einschließt. Dies kann durch die Migration auf ein neues Gerät (z. B. auf einen sicheren virtuellen Computer oder einen Computer

mit Festplattenverschlüsselung) geschehen, ohne dass ein inkompatibles Update für I2P vorbereitet oder freigegeben wurde. Daher muss der Benutzer seine Adressbucheinträge erneut ausfüllen.

2.6. Lokalisieren des I2P-Knotens nach Netzwerkleistung

Die Verwendung von Denial-of-Service-Angriffen gegen I2P-Netzwerke wurde von Kack (2012) vorgeschlagen. Bei Angriffen, die als "Darkloris" bekannt sind, öffnen die böswilligen I2P-Knoten zyklisch eine große Anzahl von Verbindungen zu Diensten, die vom I2P-Zielknoten bereitgestellt werden. Diese Verbindungen werden mit dem alleinigen Zweck initiiert, die Ressourcen des Ziel-I2P-Knotens zu verbrauchen, werden jedoch von den schädlichen Knoten niemals ordnungsgemäß verwendet oder beendet.

Kack hat erfolgreich die Wirksamkeit dieses Angriffs auf den Jetty-Webserver demonstriert, der von neuen Standardinstallationen der I2P-Routersoftware verwendet wird. Obwohl Kack seinen Angriff von einem einzigen böswilligen I2P-Knoten aus ausführte, konnte der Zielknoten keine eingehenden Verbindungen zu seinem Webserver verarbeiten, was dazu führte, dass alle neuen Eepsite-Besucher eine Fehlerseite erhielten, wie in Abbildung 3 dargestellt.

Die ursprüngliche Version des von Kack verwendeten Denial-of-Service-Angriffs wurde durch die Einführung des Anforderungs-Ratelimiters in der I2P-Routersoftware entschärft. Dieser Ansatz ist jedoch unzureichend und schützt I2P-Knoten nicht vor anderen Arten von Denial-of-Service-Angriffen. Anstelle der Webserverdomäne kann sich der Angriff stattdessen auf die Sättigung des I2P-verschlüsselten Tunnellimits, der Bandbreite oder anderer Ressourcen des I2P-Knotens konzentrieren. Der Anforderungsratenbegrenzer kann umgangen werden, da er sich auf die I2P-Netzwerkkennung des angreifenden Knotens stützt, die nicht permanent zugewiesen ist und vom Angreifer geändert werden kann, sobald sein Knoten auf die schwarze Liste gesetzt wird (Abbildung 4).

Nach dem ersten Denial-of-Service-Angriff auf den I2P-Dienstknoten bestand die erwartete Reaktion seines Betreibers darin, das Verhältnis der auf dem I2P verfügbaren Systemressourcen zu erhöhen. Dazu gehört die Erhöhung der zulässigen Gesamtbandbreite, des Tunnelgrenzwerts und der Speichergröße innerhalb der I2P-Routerkonfiguration -Ration. Auf diese Weise kann der I2P-Router jedoch noch größere Denial-of-Service-Angriffe ausführen, die sich auf den I2P-Router auswirken können. Die vom Host verwendete Netzwerkausrüstung ist der erste Kandidat für einen Ausfall. Das P2P-Konzept von I2P bedeutet, dass ein aktiver I2P-Router ständig eine große Anzahl von eingehenden TCP- und UDP-Paketen aus einem ähnlich großen Pool von eindeutigen Remote-IP-Adressen empfängt Wenn sich die Netzwerkleistung oder -verfügbarkeit ändert, kann dies mit dem Ausfall des Dienstes in Verbindung gebracht werden.

Eine Untersuchung des I2P-Netzwerks ergab, dass ungefähr die Hälfte aller I2P-Netzwerkknoten nicht länger als eine Woche verbunden bleibt (Liu et al., 2014). Dieses Verhalten lässt darauf schließen, dass eine große Anzahl von Knoten vorhanden ist, die über DSL- oder mobile Breitbandverbindungen in Wohngebieten betrieben werden und die nicht in der Lage sind, die große Anzahl von P2P-Paketen ordnungsgemäß zu handhaben, und die für diese Art von Angriffen geeignet sind.

Die erste Stichprobe von IP-Adressen, die überwacht werden müssen, wird durch Analysieren der I2P-Floodfill-Datenbank abgerufen, die von jedem I2P-Floodfill-Router gespeichert wird. AdrianCrenshaws Forschungen zur Identifizierung entfernter Eep-Sites haben eine Reihe von Python-Skripten zum Extrahieren dieser Informationen hervorgebracht (Crenshaw, 2011).

Gewöhnliche Knoten, die keine Floodfill-Router sind, können aus der Kandidatenliste entfernt werden, wodurch die Gesamtliste der Kandidaten auf eine überschaubare Anzahl (mehrere Hundert) reduziert wird. Dies liegt an der Art und Weise, wie I2P die Beförderung von normalen Routern zu Floodfill-Knoten bestimmt. Ab Version 0.9.23 kann jeder I2P-Router, der eine ausreichende Bandbreite für die Netzwerkfreigabe zulässt, in den Floodfill-Knoten wechseln. Ein Knoten, der nach dem ersten Denial-of-Service-Angriff verfügbar blieb, ist daher mit hoher Wahrscheinlichkeit verfügbar afloodfill-Knoten und in der extrahierten Liste vorhanden.

Falls erforderlich, kann die Kandidatenliste durch kontinuierliche Überwachung der Verfügbarkeit von Floodfill-Knoten und der Zuordnung nach IP weiter reduziert werden. Jeder Knoten, der nicht erreichbar ist, während der gewünschte I2P-Dienst noch online ist, ist nicht mehr aktuell. Geografische Filterung wird möglich, wenn Informationen über den anvisierten Knotenbetreiber aus anderen Quellen bekannt sind: Social Engineering, Zeitstempel oder versehentliche Veröffentlichung von Informationen. Alle Aufzeichnungen von Floodfill-Routern in NetDB haben ihre IP-Adressen gespeichert und können daher neu zugeordnet werden (Timpanaro et al., 2012).

Die verbleibenden verdächtigen Knoten-IP-Adressen können dann auf Anzeichen einer Änderung der Netzwerkleistung wie verworfene Pakete und verlängerte Umlaufzeiten überwacht werden. Die angreifenden Knoten im I2P-Netzwerk können angewiesen werden, zyklisch eine Verbindung mit der verdächtigen Eep-Site oder einer anderen Ressource herzustellen und diese zu trennen, um erzeugen ein sichtbareres Muster von Änderungen über einen längeren Zeitraum.

3. Verwandte Arbeiten

Freenet (Wei et al., 2012) ist ein unstrukturiertes P2P-System, das zum Austausch von Informationen zwischen Benutzern entwickelt wurde. Es ermöglicht das Veröffentlichen und Abrufen von Inhalten auf anonyme Weise,

wobei die Quelle und Bestimmung der Informationen Dritten und Systemservern vorenthalten wird. Peers im Netzwerk beteiligen sich an Abfragen, Speichern und Abrufen von Daten.

Freenet überträgt stattdessen keine Verantwortung für Dokumente an bestimmte Knoten. Suchvorgänge werden durchgeführt, indem nach zwischengespeicherten Kopien gesucht wird. Freenet strebt eine flatInternet-Topologie an. Mit anderen Worten, eine IP-Adresse von nebenan kann kommuniziert werden. auf die gleiche Weise würde man mit einer anderen IP auf der anderen Seite des Planeten kommunizieren, ohne entdeckt zu werden. Es wurde erstmals von einer großen Community von Online-Nutzern genutzt, um urheberrechtlich geschütztes Material im Internet zu verbreiten, ohne entdeckt zu werden. Clarke (1999) behauptet, dass dies nicht der Zweck des Projekts war. Sie diskutieren, dass das Internet die größte Bastion der Redefreiheit ist, da die Regierungen versuchen, den Informationsfluss in der Presse, im Multicasting und in gedruckten Materialien zu unterbinden. Freenet-Knoten werden verschlüsselt und durch andere Knoten geleitet, um es extrem schwierig zu machen, sowohl den Urheber als auch den Inhalt zu bestimmen (Clarke, 1999). Eine Schlüsselanforderung wird mithilfe eines Flooding-Algorithmus weitergeleitet, der die entsprechenden Daten zurückgibt. Diese Schlüssel sind ortsunabhängig. Wenn eine empfangene Datei bekannt ist, leitet sie diese an das Ziel weiter, an dem sich die Informationen befinden. Wenn der Knoten die Zieladresse nicht kennt, leitet er sie an einen Knoten weiter, der möglicherweise die Informationen enthält, oder es ist wahrscheinlich, dass er den Aufenthaltsort der Ressource kennt.

Um das Routing effizienter und intelligenter zu gestalten, verwendet Freenet historische Informationen und Statistiken aus früheren Routing-Erfahrungen, um eine entscheidungsbasierte Schätzung der Zeit zu erstellen, die erforderlich ist, um das Ziel zu erreichen. Das auf der Spezialisierung der Knoten basierende Caching sammelte die Informationen, die es dann zur Folge hatte. Greenet wurde im Juli 2003 nicht mehr mit überwältigenden Anforderungen fertig und brach zusammen. Zu diesem Zeitpunkt behandelte der Designer die Lastausgleichsprobleme, indem er die einheitliche Lastverteilung sicherstellte und Abfragen einschränkte um das festgelegte Kontingent beizubehalten. In Anbetracht dessen, dass dieser Ansatz das Problem behoben hat und effektiv funktioniert, kann er jedoch zu Funktionsproblemen führen, indem eingehende Anforderungen zum Abrufen von Ressourcen begrenzt werden. Dies bedeutet, dass sich einzelne Knoten, die sich anders als erwartet verhalten, auf den Lastausgleich auswirken und die Anforderungsfehlerrate erhöhen können. Die Herausforderung in Bezug auf Skalierbarkeit und Leistung bleibt daher auch in der Freenet-Struktur bestehen. Wie jedes andere P2P-System können Knoten in Freenet eine doppelte Rolle spielen und sind namentlich nicht unterscheidbar. Diese Komponente des Systems verbessert die Anonymität. Ein Angreifer kann jedoch mithilfe eines Paketanalysators die Verkehrslast leicht identifizieren und

Serverknoten unterscheiden. Freenet bleibt jedoch eines der wichtigsten Systeme für die Anonymisierung der Benutzer.

Der Onion Router (Tor) ist ein verteiltes Overlay-Netzwerk zur Anonymisierung von TCP-basierten Anwendungen wie Instant Messaging, Webanwendungen und Secure Shell (Dingle-dine, Mathewson & Syverson, 2004). Jeder Knoten in torchooses einen Pfad, bauen Sie eine Schaltung mit seinen Nachbarn als Nachfolger und Vorgänger bekannt. Der Datenverkehr wird über Schaltkreise mit fester Größe weitergeleitet und an jedem Knoten per Symbolschlüssel entpackt, ähnlich den Schichten einer Zwiebel. Durch die inkrementelle Weitergabe von Nachrichten wird eine vollständige Anonymität gewährleistet. Die Verwendung von Verschlüsselung auf jeder Ebene gewährleistet die Datenintegrität. Um jedoch die Änderung durch Knoten zu vermeiden, verschlüsselt Tor die Nachrichten, bevor sie den Quellknoten verlassen. Bei Tor wurden jedoch einige Schwächen festgestellt (McCoy et al., 2008; Ehlert, 2011). AdWords-Kunden können die Tornoden an den Eintrittspunkten angreifen.

Ähnlich wie I2P ist Tor anfällig für CPU-lastige Denial-of-Service-Angriffe. Tor bietet jedoch eine niedrige Latenz und eine hohe Bandbreite, was es für Benutzer attraktiv macht, die Sofortnachrichten und große Dateien gemeinsam nutzen. Die in tor auftretenden Probleme können verwendet werden, um die Benutzer zu anonymisieren oder die übertragenen Nachrichten zu entschlüsseln. Dies würde jedoch den Rahmen dieses Papiers sprengen. Trotzdem bleibt Tor wie jeder andere Anonymitätsdienst im Internet eine Herausforderung bei jeder forensischen Untersuchung.

4. Fazit und zukünftige Arbeiten

In diesem Artikel wurden spezifische Sicherheitsaspekte und Schwachstellen von I2P-Netzen erörtert. Darüber hinaus wurden die Funktionalität und ihre Funktionen beschrieben. Als solches wurde ein Argument vorgebracht, dass I2P zwar die Möglichkeit bietet, die Vertraulichkeit und den Datenschutz der Benutzer zu wahren, aber im Allgemeinen für illegale Aktivitäten ausgenutzt und genutzt wird. Während die Anonymitätssysteme die Privatsphäre der Benutzer wahren, die Meinungsfreiheit fördern und den freien Informationsfluss erleichtern, gibt die Ebene illegaler und krimineller Aktivitäten in I2P-Netzwerken weiterhin Anlass zur Besorgnis. Aufgrund der technologischen, geopolitischen und rechtlichen Herausforderungen ist der Zugang zu Informationen über solche Aktivitäten ein Problem für die forensischen Analysten und Strafverfolgungsbehörden. Daher haben wir in diesem Artikel verschiedene Techniken bereitgestellt, die auf den Schwachstellen und Mängeln im I2P-Netzwerk basieren (Zantout & Haraty, 2011), um I2P-Artefakte forensisch zu identifizieren und abzurufen. Unsere Analysen und Experimente zeigen, dass solche Lösungen in die branchenweit anerkannten forensischen Tools integriert werden können, um eine bessere Praxis bei I2P-Untersuchungen

innerhalb der Strafverfolgung zu fördern und die Kontinuität der Nachweise zu verbessern.

Für zukünftige Arbeiten werden wir die Sicherheitsabläufe von I2P genauer untersuchen, um ein vollständigeres Verständnis des gesamten Netzwerks zu ermöglichen. Dies wird zu einer effektiven und effizienten Untersuchung von I2Pactivities beitragen und einen umfassenden Ansatz für die forensische Analyse der schädlichen Artefakte liefern.

Anmerkungen

1. Skype - https://www.skype.com/en/
2. BitTorrent - www.bittorrent.com/
3. Freenet - freenetproject.org
4. www.icann.org

Offenlegungserklärung

Von den Autoren wurde kein potenzieller Interessenkonflikt gemeldet.

Referenzen

Braun, P. J., Ekler, P., & Fitzek, F. (2016).
Network coding enhanced
browser based Peer-to-Peer streaming
. 2016 IEEE International
Conference on Systems, Man, and Cybernetics (SMC). IEEE.
Clarke, I. (1999). Freenet: A distributed anonymous information
storage and retrieval system. Retrieved from
http://freenet
project.org/freenet.pdf
Coudriau, M., Lahmadi, A., & Francois, J. (2016).
Topological anal-
ysis and visualisation of network monitoring data: Darknet case
study
. IEEE International Workshop on Information Forensics
and Security. IEEE.
Crenshaw, A. (2011). Darknets and hidden servers: Identifying
the true IP/network identity of I2P service hosts. Retrieved
from
http://www.irongeek.com/downloads/Identifying%
20the%20true%20IP%20of%20I2P%20service%20hosts.pdf
Dingledine, R., Mathewson, N., & Syverson, P. (2004).
Tor:
The second-generation onion router
. Proceedings of the13th
USENIX Security Symposium.
Ehlert, M. (2011). I2P usability vs. tor usability: A bandwidth
and latency comparison. Retrieved from
http://userpage.fu-
berlin.de/semu/docs/2011_seminar_ehlert_i2p.pdf
Hesselman, C., Moura, G. C. M., de Oliveira Schmidt, R., & Toet,
C. (2017). Increasing DNS security and stability through a

control plane for top-level domain operators.
IEEE Communi-
cations Magazine
,
55
, 197–203.
Jawad, M., Serrano-alvarado, P., & Valduriez, P. (2013). Support-
ing data privacy in P2P systems. Table of Contents (pp. 1–51).
Jayashree, G., & Perumal, V. (2014).
Enhancing similarity based
query searching performance using self-organized semantic
overlay networks
. 2014 International Conference on Com-
puter Communication and Systems. IEEE.
Kack, C. (2012). Layer 7 DOS against I2P darknet. Retrieved
from
http://blog.kejsarmakten.se/all/projects/2012/09/11/
dark-loris.html
Liu, P., Wang, L., Tan, Q., Li, Q., Wang, X., & Shi, J. (2014). Empiri-
cal measurement and analysis of I2P routers. Retrieved from
https://pdfs.semanticscholar.org/3e5f/2b136df32beef1281b
6b2f206093806c57f6.pdf
McCoy, D., Bauer, K., Grunwald, D., Kohno, T., & Sicker, D. (2008).
Shining light in dark places: Understanding the tor network
.
Proceedingsof Privacy Enhancing Technologies Symposium
(PETS), Leuven, Belgium.
Nadeem, M. A., & Karamat, T. (2016).
A survey of cloud net-
work overlay protocols
. 2016 Sixth International Conference
on Digital Information and Communication Technology and
its Applications (DICTAP). IEEE.
Timpanaro, C., Chrisment, I., & Festor, O. (2012). A bird’s eye view
on the I2P anonymous file-sharing environment. Retrieved
from
https://hal.inria.fr/hal-00744919/PDF
Valdez, J., Guirguis, M., Wingate, D., & Rinkevich, R. (2011). An
expanding reference library for Peer-to-Peer content. eCrime
Researchers Summit (eCrime), 2011. IEEE.
Wei, Y., Wang, C., Chu, Y., & Chang, R. (2012). A secure and
stable multicast overlay network with load balancing for scal-
able IPTV services.
International Journal of Digital Multimedia
Broadcasting
,
2012
(pp. 1–12.B).
Zantout, B., & Haraty, R. (2011).
I2P data communication system
.
Proceedings of ICN.

https://doi.org/10.1080/21642583.2017.1331770
Crossmark: https://crossmark.crossref.org/dialog/?doi=10.1080/21642583.2017.1331770&domain=pdf&date_stamp=2017-06-12