匿名通信システムの攻撃手法に関する調査

青木 太一† 青木 卓矢† 佐藤 直†
島田 要‡ 山口 信幸‡ 髙橋 正樹‡

†情報セキュリティ大学院大学情報セキュリティ研究科
〒221-0835 神奈川県横浜市神奈川区鶴屋町 2-14-1
{ dgs148101, mgs141103, sato }@iisec.ac.jp

‡警察大学校サイバーセキュリティ研究・研修センター
〒183-8558 東京都府中市朝日町 3-12-1
{ k.shimada, n.yamaguchi, takahashi }@nparc.ac.jp

あらまし Torに代表される匿名通信システムはプライバシーの保護を実現する有益な技術である。一方で、サイバー犯罪やマルウェア通信などにも悪用され、攻撃者にとって有利な状況も作り出している。Torの匿名性を解除するde-anonymize手法は、これまでにも数多くの研究がなされているが、無条件かつ安定的に成功している手法は存在しない。そこで本稿では、Torを中心に匿名通信システムに対する既存研究をサーベイし、Torに対する攻撃アプローチとしてまとめた上で、Torのde-anonymizeに対する課題について考察した。

A Survey about attack methods of Anonymous-Communication Systems

Taichi Aoki† Takuya Aoki† Naoshi Sato†
Kaname Shimada‡ Nobuyuki Yamaguchi‡ Masaki Takahashi‡

†Institute of Information Security
2-14-1 Tsuruya-cho, Kanagawa-ku, Yokohama, Kanagawa, 221-0835, Japan
{ dgs148101, mgs141103, sato }@iisec.ac.jp

‡National Police Academy Cyber Security Research-Training Center
3-12-1 Asahi-cho, Fuchu, Tokyo, 183-8558, Japan
{ k.shimada, n.yamaguchi, takahashi }@nparc.ac.jp

Abstract An anonymous communications system represented by Tor is the useful technology which achieves private protection. On the other hand, it's profitable for an attacker, when it's abused by a cybercrime and malware communication. De-anonymous technique to Tor exists much. But a method that is unconditional and stable, doesn't exist. So in this paper, we surveyed an existence study of Tor, and, it was put in order as de-anonymous approach to Tor in an anonymous communications system. And, it was considered about problem to de-anonymous approach of Tor.

1　はじめに

インターネットの普及に伴い、通信における通信者のプライバシーの保護や、通信の検閲から身を守るといった発信者匿名化に対する需要が増えている。

標準的なインターネット通信においては、IP アドレスを知ることで送受信者が一意に特定される性質を持つ。匿名通信システムは、その IP 通信においても、本来の情報発信者の特定を困難にすることを目的とした技術である。

匿名通信システムの代表的な実装である Tor[1]は、その開発国であるアメリカや、プライバシーに関心の強いヨーロッパを中心に、世界的に広く使われている[2][3][4]。一方、匿名通信システムは、その匿名性の強力さと利用の手軽さから、サイバー犯罪[5]やボットネットマルウェア通信への悪用[6]など、犯罪の温床にもなっている[7][8]。

匿名通信システムに対してその匿名性を解除することを de-anonymize と呼び、これまでにも世界的に多くの研究が行われている。しかしながら、Tor に対する de-anonymize に着目すると、現在においても無条件かつ安定的に成功している研究は存在しない。

本稿では、これまで匿名通信システムに対して行われてきた攻撃手法を俯瞰的に整理し、Tor に対する攻撃アプローチとしてまとめることで、Tor に対する攻撃の課題を再認識するとともに、Tor の持つ匿名性に対する考察を行う。

2　匿名通信システム

匿名通信システムには様々な仕組みの方式が考案されている[9][10][11]が、ここでは、オーバーレイネットワークとして実装されている匿名通信システムとして代表的な Tor[1][12]について紹介する。

2.1　Tor

米海軍調査研究所の支援によって開発されたオニオンルーティングによる匿名化技術のリファレンス実装である。電子フロンティア財団によって支援され、一般に使われるようになった 2004 年以来、10 年以上も破られていない堅牢な匿名システムである。受信者に対する発信者の匿名化には、古くは Proxy 技術が使われていた。Tor はその Proxy 技術を大きく発展させた多段 Proxy システムととらえることが出来る。それぞれの Tor 中継ノードは SOCKS Proxy として動作する。オニオンルーティングの名称の元となる玉ねぎの皮のように、中継ノード（Onion Router: OR）を経由するたびに通信内容を多重に暗号化・または復号しながら転送する仕組みが大きな特徴である。暗号化されたパケットを中継している OR ノードは、自身の前後の通信相手しか知ることが出来ず、中継ノードに対する本来の発信者および受信者の情報は暗号化されているため知ることが出来ない仕組みによって匿名性を維持している。Tor の実装は、中継ノードに対する送受信者の匿名性を提供するシステムであり、通信内容に対する匿名性は考慮されていない。Tor からインターネットへ接続する Exit ノードと呼ばれるノードでは、通信内容は平文として見ることが可能であるため、通信内容を秘匿化するには SSL 等で適切に暗号化する必要がある。Tor で提供される主な機能としては①匿名通信を行う機能、②TCP ベースの匿名サービスを提供する機能の2つがある。後者は Hidden Service と呼ばれる。Hidden Service では、半角英数 16 文字の末尾に.onion を付けたドメインがアドレスとして用いられる。Hidden Service のノードの特定には、P2P の技術（分散ハッシュテーブル: DHT）をベースとしたアドレス解決機能が使われている。

3　攻撃手法と目的別の分類

ここでは、Tor に対する攻撃手法を既存研究から拾い上げ、その概要を紹介する。攻撃名称については I2P Project による脅威モデル[13]をベースとして用い、その目的別に独自に分類している。匿名システムに対する攻撃の分類に関する研究としては、Lu らによる先行研究[14]があり、そこでは攻撃の性質が受動的か能動的かの観点で分類されている。

3.1　分析手法として使われるもの

(a) Traffic analysis attacks [15]

トラフィック分析攻撃と呼ばれる。ネットワークトラフィックを観測することで経路を推定する手法。主にトラフィック量とその時間変化のベクトルを相関させることが多いが、独自の特徴ベクトルを用いる場合もある。

(b) Deep packet inspection [16]

ネットワークパケット中に含まれる情報を使用すること全般を指す。パケットが平文である場合に有効な手法。匿名システムの場合、上位レイヤーは暗号化されていることが多いため、レイヤーの低いプロトコルに対して使用される。

3.2 トラフィック分析攻撃で使われるもの

(c) Intersection attacks [13]

攻撃者によって配置された中継ノードを経由させる攻撃。もし中継した匿名ネットワークの両端が攻撃者のノードであった場合、トラフィック分析攻撃等によって発信者ノードを絞り込むことが出来る。トラフィック分析を使う多くの研究で使われる。

(d) Collusion attacks [14]

複数の中継ノードから得られる情報を使い、より精度の高い分析を行う攻撃。トラフィック相関を使う研究では、あらかじめ結託させた入口ノードと出口ノードまたは宛先サーバから得られる 2 点間の情報を使用して特徴量を相関させる手法が多い。

(e) Brute force attacks [17]

この攻撃は、任意のノードに対してメッセージを大量に送信することで成立する。DoS 攻撃として機能する他にも、ノードのトラフィック量を観察し、想定される大量のトラフィックが届かないノードを除外していくことで、発信者ノードを絞り込むことができる。

(f) Tagging attacks

トラフィックに識別情報を付与し、発信者ノードを絞り込む攻撃。Deep packet inspection と組み合わせて使われることが多い。Tor 経由のダウンロードファイルにマルウェアを含ませる攻撃が観測されているとの報告もある[18]。

(g) Fingerprinting attacks[19][20]

パケット数やサイズなど、サーバ毎に固有の応答を返すパラメータを指紋情報として蓄積し、接続先のサーバを推定する攻撃。同時に複数の web アクセスを行う等のダミートラフィックを流すことで解析を妨害する anti de-anonymize 手法も存在する。

(h) Timing attacks[21][22]

時間差をつけたレスポンストラフィックを送り込み、観測ノード上で得られたトラフィック量の時間変化グラフの相関を取ることで経路を推定する。トラフィック分析攻撃のひとつ。

(i) Predecessor attacks[23]

攻撃者のノードを多数配置してノードとの接続頻度の統計を取ることで、接続頻度の高いノードをクライアントノードとして推定する攻撃。

(j) Distance attacks [24]

サーバ側とクライアント側で現れる TCP レスポンスタイムの時間差を求め、発信者ノードを絞り込む攻撃。タイミング攻撃と似ているが、この攻撃では個々のパケットに着目する。

(k) Remote-Traffic analysis [25]

Tor とは無関係にインターネット経由で送受信したパケットのラウンドトリップタイム(RTT)を用いて、相手のトラフィック量を推定する攻撃。サイドチャネル攻撃のひとつ。

(l) Anti-Transform attacks [26]

システムを経由することで変化するトラフィックパターンに対し、機械学習を用いて元のトラフィックパターンを復元する攻撃。トラフィック相関時の識別率が良くなる。

3.3 攻撃者のノードへ誘い込むことを目的としたもの

(m) Sybil attacks [27]

ネットワーク内に大量の攻撃ノードを送り込み、ネットワークの占拠を図る攻撃。結託攻撃と同義に扱われる。ネットワーク内に攻撃者のノードが増えると、交差攻撃が成功する確率が高まる。小規模なネットワークに対して有効。

(n) Denial of service attacks [1]

大量のメッセージを送信して、匿名ネットワーク全体や、特定のノードをダウンさせる攻撃。ブルートフォース攻撃によって実現する他にも、システムの脆弱性を突いて機能停止に追い込む場合もある。正規ノードを DoS 攻撃でダウンさせて攻撃者のノードへ誘い込む手法にも使われる。

(o) Flooding attacks [13]

大量のリソース要求を発生させ、ネットワーク資源をあふれさせる攻撃。DoS 攻撃のひとつ。

(p) Starvation attacks [13]

ネットワーク内に攻撃ノードを多数配置し、意図的に適切な動作をさせないことで機能不全を起こす攻撃。DoS 攻撃のひとつ。

(q) Sniper attacks [28]

狙った中継ノードに対して輻輳を発生させ、TCP フロー制御の動きによって特定のノードの中継能力を実質的に停止させるサービス不能攻撃。

(r) TCP replay attacks [29]

受信した TCP パケットを再送し、受信ノードの TCP カウンタエラーを発生させる攻撃。DoS 攻撃のひとつ。

(s) TCP reset attacks [13]

特定のノードに TCP リセットパケットを送信し、コネクションを意図的に終了させるサービス不能攻撃。

(t) Partitioning attacks [13]

ターゲットと正規のノードと間の接続を切り離し、ターゲットを攻撃者のノードに誘い込む攻撃。TCP リセット攻撃などと組み合わせて使われる。

3.4 システム固有の機能に対する攻撃

(u) Harvesting attacks [30]

公開されている情報から、有益な情報を収集する攻撃。例えば、ネットワーク内のノードの一覧などを取得する。

(v) Central Resource attacks [1]

システムの中で単一のものとして集中している機能を狙った攻撃。Tor においてはディレクトリサーバに対する攻撃として知られる。

(w) Cryptographic attacks [31]

使用されている暗号システムの脆弱性を狙い、暗号を解除することによって匿名性の解除を試みる攻撃。

3.5 システムの外で行われる攻撃

(x) Development attacks [13]

開発パッケージを改竄し、脆弱な実行ファイルが生成されるように仕向ける攻撃。

(y) Implementation attacks [13]

システムの実装の不備を利用した攻撃。脆弱性攻撃とも呼ばれる。

3.6 実装攻撃の例

(z) Quantum cookie attacks[32][33]

TorBrowser のベースとなる FireFox ブラウザの脆弱性を利用して de-anonymize に成功した例。サーバからの要求によって、ブラウザに保存された Yahoo や Hotmail、DoubleClick 広告識別子などの cookie 情報が取得出来てしまう不具合を利用して、取得したメールアカウント等の情報から発信者を特定することが出来た。この脆弱性は 2012 年 11 月に修正されている。

(aa) JavaScript や Flash を使った攻撃[1][34]

ブラウザ上で動作する JavaScript などから匿名ではない通常の通信を行い、発信者を特定することが出来る。匿名通信システムを使う場合にはこのような機能を使用しないことが推奨されている。

(bb) DNS を使った攻撃[1][35]

Tor の初期の実装では、DNS リクエストに匿名ではない通常の通信が行われていたため、DNS リクエストを解析することで発信者を特定することが出来た。現在は DNS リクエストも Tor 内部によって解決するようになっている。

3.7 その他の事例

(cc) Operation Onymous

FBI(米国連邦捜査局)と Europol(欧州刑事警察機構)による、Silk Road 2.0 を含む Tor 経由の匿名ドメイン 400 件の差し押さえに成功した事例が存在する。Tor に対する世界初の大規模な摘発事例と言われている。具体的な手法は明らかにされていないが、メールの利用や金銭の受け渡しなど、匿名システムの外で行う行動から辿られたのではないかと TorProject によって推測されている[36]。その場合はソーシャルハッキングに分類できる。

4 攻撃手法の考察と課題

匿名通信システムに対する既存の攻撃手法を攻

撃位置の観点で分類したものが図[Figure1]である。図の上半分は、匿名システム固有の仕様や動作上の仕組みを使った攻撃であり、ホワイトボックスタイプの攻撃アプローチとしてとらえることが出来る。図の下半分はトラフィック分析と、その分析精度を高めるための攻撃手法であり、TCP/IP や HTTP 等の仕組みが使われる、いわばブラックボックスタイプの攻撃アプローチである。ホワイトボックスタイプのアプローチは、攻撃成功時に発信者を特定する精度が高い反面、攻撃手法自体に脆弱性やシステムの設計の不備を利用していることから、匿名システム側で何らかの対策がなされてしまうことにより de-anonymize が封じられるリスクがある。対してブラックボックスタイプのアプローチでは、TCP/IP の仕組みから得られる情報を活用しているため、インターネットのオーバーレイとして実装される匿名システムとしてはその解析対策をとることは難しく、攻撃手法が長く利用できるメリットがある。一方で、トラフィック量などを観測するためには、観測用の攻撃ノードを匿名ネットワーク内部に投入するか、中継ルータなどからトラフィック量を得る必要がある。特に、中継ルータからトラフィック量を得ようとすると、技術的には①観測点が多すぎる問題があることや、社会的には②解析実施国のプライバシーに関する法律の他、③中継ノードが国境を超えることによる国際連携の難しさの点から実現の難易度は高い。トラフィック分析を利用した既存研究では、これらの問題点を回避するため、攻撃ノードを経由する通信であることをその分析対象の前提とされている。図右上の分類は、ターゲットを攻撃ノードに効率的に接触させるための間接的な攻撃手法と、トラフィックをリモートから推定する手法をそれぞれ分類している。

Tor が広く使われて 10 年以上経つにもかかわらず、未だに決定的な de-anonymize 手法は見つかっていない。Tor では、匿名システムとしての不正ノードが仮に浸透した場合も、人手で排除する運用が正しく機能している点、そして、ネットワーク検閲と国際連携の難しさという社会環境を、匿名性の根拠のパラメータとして設計に上手く取り入れた点が、Tor の匿名化技術としての堅牢さであるといえるだろう。

5 まとめ

本稿では、オーバーレイネットワークとして実装されている匿名通信システムとして代表的な Tor に対する攻撃手法を既存研究からピックアップし、その目的別に分類を試みた。匿名通信システムに対する匿名性を解除するための de-anonymize 手法には、ホワイトボックスタイプのアプローチとブラックボックスタイプのアプローチが存在し、後者においてはトラフィック分析攻撃にその手法が集約されていることがわかった。

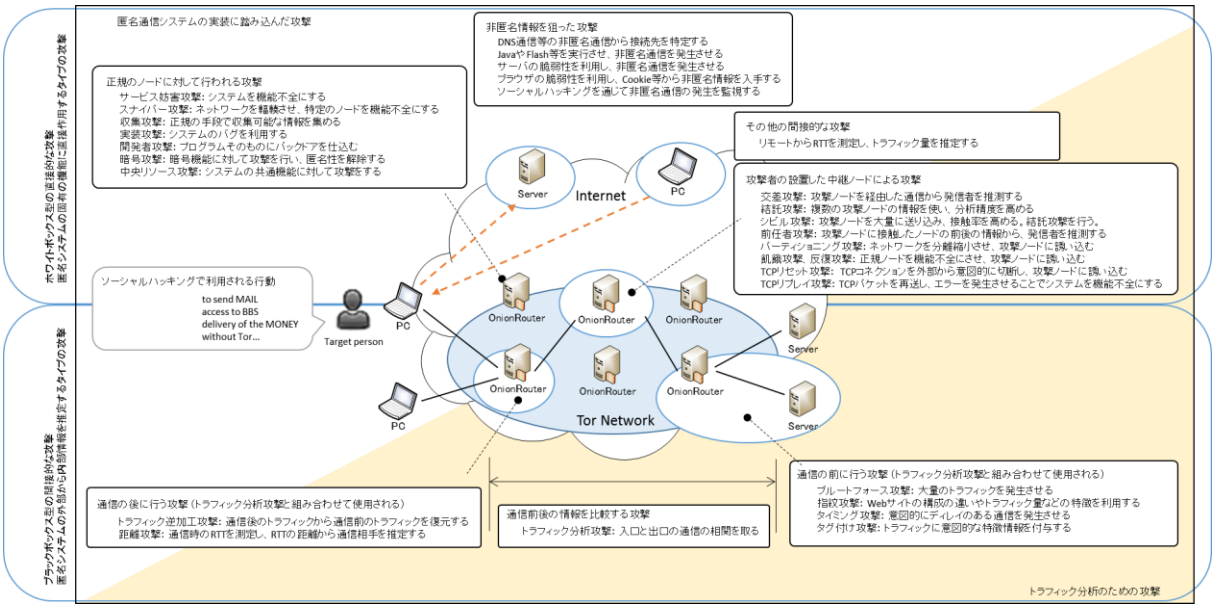

Figure 1 攻撃手法の目的別分類

参考文献

[1] Dingledine, Roger, Nick Mathewson, and Paul Syverson. Tor: The second-generation onion router. Naval Research Lab Washington DC, 2004.

[2] 土屋大洋, "デジタル時代の合法的通信傍受", ネット・ポリティックス 2001, 2001, pp.16-20

[3] Wikipedia: Tor (anonymity network), https://en.wikipedia.org/wiki/Tor_%28anonymity_network%29, 2015.07.20

[4] Tor Project: How to handle millions of new Tor clients, https://blog.torproject.org/blog/how-to-handle-millions-new-tor-clients, 2015.07.20

[5] Wikipedia: パソコン遠隔操作事件, https://ja.wikipedia.org/wiki/%E3%83%91%E3%82%BD%E3%82%B3%E3%83%B3%E9%81%A0%E9%9A%94%E6%93%8D%E4%BD%9C%E4%BA%8B%E4%BB%B6, 2015.07.20

[6] Casenove, Matteo, and Armando Miraglia. "Botnet over Tor: The illusion of hiding." Cyber Conflict (CyCon 2014), 2014 6th International Conference On. IEEE, 2014.

[7] Bergman, Michael K. "White paper: the deep web: surfacing hidden value." Journal of electronic publishing 7.1 (2001).

[8] Ciancaglini, Vincenzo, et al. "the Deep Web.", 2015

[9] Project: AN.ON, http://anon.inf.tu-dresden.de/desc/desc_anon_en.html, 2015.07.20

[10] Wikipedia: Java Anon Proxy, https://en.wikipedia.org/wiki/Java_Anon_Proxy, 2015.07.20

[11] Wikipedia: I2P, https://en.wikipedia.org/wiki/I2P, 2015.07.20

[12] Tor Project: Anonymity online, https://www.torproject.org/, 2014.01.29

[13] I2P'S THREAT MODEL, https://geti2p.net/ja/docs/how/threat-model, 2015.07.20

[14] Lu, Tianbo, et al. "Towards Attacks and Defenses of Anonymous Communication Systems." International Journal of Security and Its Applications 9.1 (2015): 313-328.

[15] Murdoch, Steven J., and George Danezis. "Low-cost traffic analysis of Tor." Security and Privacy, 2005 IEEE Symposium on. IEEE, 2005.

[16] Chaabane, Abdelberi, Pere Manils, and Mohamed Ali Kaafar. "Digging into anonymous traffic: A deep analysis of the tor anonymizing network." Network and System Security (NSS), 2010 4th International Conference on. IEEE, 2010.

[17] Li, Chenglong, et al. "Super nodes in Tor: existence and security implication." Proceedings of the 27th Annual Computer Security Applications Conference. ACM, 2011.

[18] Leviathan security group: (The Case of the Modified Binaries), http://www.leviathansecurity.com/blog/the-case-of-the-modified-binaries, 2015.07.20

[19] Panchenko, Andriy, et al. "Website fingerprinting in onion routing based anonymization networks." Proceedings of the 10th annual ACM workshop on Privacy in the electronic society. ACM, 2011.

[20] Abbott, Timothy G., et al. "Browser-based attacks on Tor." Privacy Enhancing Technologies. Springer Berlin Heidelberg, 2007.

[21] Perry, Mike. "Securing the tor network." Proc. of Black Hat (2007).

[22] Chakravarty, Sambuddho, et al. "On the Effectiveness of Traffic Analysis Against Anonymity Networks Using Flow Records." Passive and Active Measurement. Springer International Publishing, 2014.

[23] Wright, Matthew, et al. "Defending anonymous communications against passive logging attacks." Security and Privacy, 2003. Proceedings. 2003 Symposium on. IEEE, 2003.

[24] Overlier, Lasse, and Paul Syverson. "Locating hidden servers." Security and Privacy, 2006 IEEE Symposium on. IEEE, 2006.

[25] Kadloor, Sachin, et al. "Low-cost side channel remote traffic analysis attack in packet networks." Communications (ICC), 2010 IEEE International Conference on. IEEE, 2010.

[26] 横手健一, and 松浦幹太. "匿名通信システム Tor の安全性を低下させるトラフィック逆加工." Computer Security Symposium. Vol. 3. 2012.

[27] Levine, Brian Neil, Clay Shields, and N. Boris Margolin. "A survey of solutions to the sybil attack." University of Massachusetts Amherst, Amherst, MA (2006).

[28] Jansen, Rob, et al. The sniper attack: Anonymously deanonymizing and disabling the Tor network. OFFICE OF NAVAL RESEARCH ARLINGTON VA, 2014.

[29] Pries, Ryan, et al. "A new replay attack against anonymous communication networks." Communications, 2008. ICC'08. IEEE International Conference on. IEEE, 2008.

[30] Snader, Robin, and Nikita Borisov. "A Tune-up for Tor: Improving Security and Performance in the Tor Network." NDSS. Vol. 8. 2008.

[31] Eric Filiol, 動的な暗号バックドアパート 2 TOR ネットワークのハイジャック, https://pacsec.jp/psj11/PacSec2011_Dynamic-Cryptographic-Backdoors_jp.pdf, 2015.07.20

[32] 浜村拓夫の世界: (Tor を破る方法), http://hamamuratakuo.blog61.fc2.com/blog-entry-978.html, 2015.07.20

[33] ars technica: (How the NSA might use Hotmail, Yahoo or other cookies to identify Tor users), http://arstechnica.com/security/2013/10/how-the-nsa-might-use-hotmail-or-yahoo-cookies-to-identify-tor-users/, 2015.07.20

[34] Wang, Xiaogang, et al. "A potential HTTP-based application-level attack against Tor." Future Generation Computer Systems 27.1 (2011): 67-77.

[35] Fleischer, Gregory. "Attacking tor at the application layer." Presentation at DEFCON 17 (2009): 54.

[36] TorProject: (Thoughts and Concerns about Operation Onymous), https://blog.torproject.org/blog/thoughts-and-concerns-about-operation-onymous, 2015.07.20