様　式　Ｃ－１９、Ｆ－１９－１、Ｚ－１９　（共通）

科学研究費助成事業　　研究成果報告書

令和　　元 年　　６ 月 １１ 日現在

機関番号：１２１０２
研究種目：基盤研究(B)（一般）
研究期間：2016～2018
課題番号：１６Ｈ０２８０５

研究課題名（和文）インターネットにおける利用者協調による利用者追跡防止

研究課題名（英文）Preventing user tracking by user collaboration on the Internet

研究代表者
新城　靖（Shinjo, Yasushi）

筑波大学・システム情報系・准教授

研究者番号：００２５３９４８

交付決定額（研究期間全体）：（直接経費）　　5,800,000円

研究成果の概要（和文）：インターネットの利用者は、ランダムに見える文字列を含む URL でコンテンツにアクセスする時、利用者追跡がなされていないことを確かめる術を持たない。本研究では、次の2つのしくみを実現し、利用者追跡を防止する。(1) 協調している利用者は、ある URL 等の識別子で識別されたコンテンツをアクセスする時、同じコンテンツをアクセスする利用者が少なくとも k 名以上存在することを利用者自身で確認可能にする。(2) 利用者による濫用を抑止しながら、IPアドレスを効果的に匿名化する。

研究成果の学術的意義や社会的意義
本研究の結果、インターネットにおける利用者追跡の考え方に大きな変革がもたらされる。従来、利用者は、Web サーバが掲げているプライバシ・ポリシーを信じるしかなかった。本研究の結果、利用者は、利用者追跡の不安から開放される。また利用者が追跡されないサーバを選択して利用するようになれば、サーバ運営者も、利用者追跡の代わりに利用者から受け入れ可能な方法を模索せざるをえなくなる。

研究成果の概要（英文）：When users of the Internet access Web contents with the URLs that contains random strings, they have no method to notice that they are not tracked with these strings. This research realizes following two mechanisms to prevent user tacking. (1) When a user accesses a Web contents with a URL, the user can know that k or more users are accessing the same contents. (2) IP addresses are hidden from the Web servers while preventing abuse.

研究分野：情報工学

キーワード：情報工学　計算機システム　ネットワーク　プライバシ保護　個人情報保護

様　式　Ｃ－１９、Ｆ－１９－１、Ｚ－１９、ＣＫ－１９（共通）

１．研究開始当初の背景

インターネットの利用者は、Web ブラウジングをするだけで、その意に反してサーバから追跡(user tracking)されている。メール・マガジンの購読でも、画像等の遠隔コンテンツを埋め込むことで、Web と同様に追跡される。利用者追跡は、サーバにとっては効果が高い広告の表示やサービスの改善といった有用性があるが、利用者にとってはプライバシの侵害となる。Web ブラウザには、標準の cookie ブロック機能や Ghostry 等の拡張機能で利用者追跡を拒む機能もあるが、不十分である。サーバにログインして閲覧するコンテンツの場合、利用者は追跡を拒む手段を持たない。追跡されている利用者がそのようなサーバにログインしてしまうと、ログイン以前のアクセスまでも特定の個人と結びつけられてしまう。

Web ページ・アクセスで利用者のプライバシを保護する研究が国内外で活発に進められている。たとえば、EU (European Union) の ABC4Trust (Attribute-based Credentials for Trust) プロジェクトで開発された手法を用いると、利用者はアクセスが限定された Web ページにアクセスする時に、個人を識別できる情報を含まない「属性リスト」だけを提示すればよい。このように属性を用いて匿名性を実現したとしても、大きな問題が残っている。それはサーバが同じコンテンツに対して「個人化された識別子」(URL)を配布することで、利用者追跡がなされてしまうことである。個人化された URL を配布する手法は、アクセスが制限されていない(誰でもアクセスできる) Web ページの閲覧を追跡する時にも利用される。利用者は、ランダムに見える文字列を含む URL でコンテンツにアクセスする時、現在、利用者追跡がなされていないことを確かめる術を持たない。

２．研究の目的

本研究では、次の 2 つのしくみを実現し、利用者追跡を防止する。

(1) 協調している利用者は、ある URL 等の識別子で識別されたコンテンツをアクセスする時、同じコンテンツをアクセスする利用者が少なくとも k 名以上存在することを利用者自身で確認可能にする。

(2) 利用者による濫用を抑止しながら、IP アドレスを効果的に匿名化する。

我々は、インターネットにおいて、 VPN (Virtual Private Network) を用いて検閲用ファイアウォールをパイパスする仕組みを実装している（引用文献①)。この仕組みの特徴は、利用者(ボランティア)が VPN サーバを実行し別の利用者を助けること、および、VPN サーバが協調することで検閲当局による探知を逃れることである。本研究では、この利用者協調の考え方を、利用者追跡防止のために用いる。

３．研究の方法

本研究では利用者追跡の防止という目的を達成するために､以下のような利用者が相互に協調するための仕組みを実装する(図 1)。

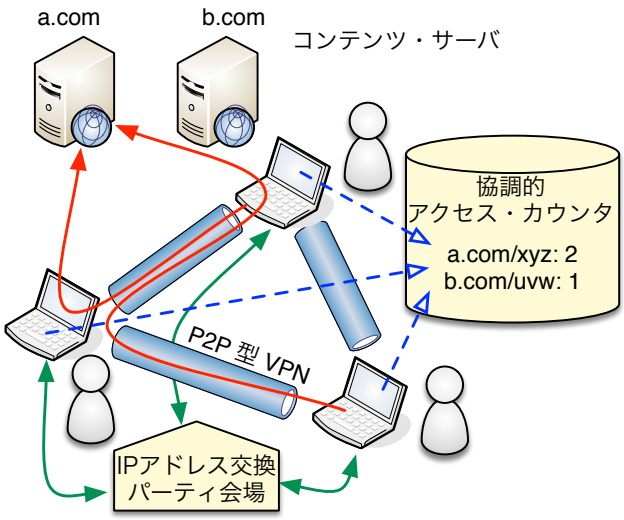

図 1　利用者協調による利用者追跡の防止

(1) 協調的アクセス・カウンタ。コンテンツの ID(identifier) ごとに、何人の利用者がいるかを集計する。この値が k 以上いれば、利用者は、同じコンテンツをアクセスする人が少なくとも k 名いることが自身で確認できる。

(2) P2P (peer-to-peer) 型の VPN。利用者の PC (Personal Computer) 間を VPN で接続する。これにより、利用者は相互に他の利用者の PC に割り振られた IP アドレスを用いて目的のコンテンツにアクセスできる。この時、アクセスできる Web サーバの IP アドレスやポート番号を制限することで、他の利用者による濫用を防ぐ。

(3) IP アドレス交換パーティ会場。これは、利用者が VPN で接続する相手の PC を見つける機能を提供するプログラムである。これを実現するために、Richard Stallman が提唱した「Charlie カード交換パーティ」の手法を用いる。Charlie カードとは、ボストン市の地下鉄に導入された Suica のような交通カードである。これは、当局が利用者の行き先を追跡できるものであった。これを嫌った Stallman は、チャージが 0 になったカードをパーティに持ち寄りランダムに交換することで、利用者追跡を防止することを考案した。本研究ではこの手法を用いて、インターネットに分散した利用者が互いの IP アドレスを交換できるようにする。

(4) Web ブラウザ。Web ブラウザは、URL を利用する前に「協調的アクセス・カウンタ」

で k 名以上いるか確認する。

４．研究成果

本研究では、協調的アクセスカウンタを DHT (Distributed Hash Table) を用いて実装した。DHT としては、WebRTC (Web Realtime Communication) によりメッセージのやり取りを行う webrtc-chord を用いた。webrtc-chord では、利用者が実行した Web ブラウザが DHT のノードとして動作する。DHT に格納する時のキーとしては、URL のハッシュ値を用いた。値としては、単純に整数を用いると、複数のノードで同時にカウントアップがなされた時に問題が生じる。この問題を解決するために、本研究では、webrtc-chord が持つ挿入機能を用いた。これは、複数の値が同時に挿入されたとしても、値が失われることはない。カウンタの値を増やす時には、ノードの ID を挿入する。カウンタの値を得るには、値のリストの長さを計測する。

この協調的アクセスカウンタを利用する Web ブラウザを、Google Chrome の拡張機能として実装した。この機能拡張は、バックグランド・ページにより、webrtc-chord のノードの機能を起動する。ユーザがページをアクセスすると、chrome.webRequest.onBeforeRequest イベントに対するハンドラにおいてそれを検出する。このハンドラは、協調的アクセスカウンタを使って、その URL のカウンタ値を取得する。設定された値以上であれば、それをそのままアクセスさせる。以下であれば、Web ブラウザ内の設定のページを表示する。ユーザは、このページで、カウンタの値を確認したり、一時的にアクセスを許可できる。

本研究では、IP アドレス交換パーティ会場を Web アプリケーションとして実装した。IP アドレスを交換したい利用者では、VPN 管理プログラムが実行され、この Web アプリケーションに HTTP 上の REST によりアクセスする。VPN 管理プログラムと Web アプリケーションの間では、 JSON Web Token (JWT) によりセッションを管理する。ノードが IP アドレスを交換する時、単純に FIFO のように交換すると、交換相手が予測可能になり、攻撃に利用されることがある。本研究では、この攻撃を防ぐために、一定数の IP アドレスを溜め、ランダムに交換するようにした。また、悪意のある利用者が自分が管理するノードで他の利用者を誘導して通信を監視する攻撃が考えられる。これは、Sybil 攻撃の一種である。本研究では、この攻撃を受けにくくするために、IP アドレスを登録する時に、Proof-of-work として重たい計算を課す。この計算は、通常の PC では、十分に問題なくこなすことができるが、大量のノードを登録しようとする攻撃者にとっては大きな負担になる。

本研究では、P2P 型 VPN を Tinc VPN を用いて実装した。VPN は、一般に、リモート・アクセス等、互いに信頼しあっているコンピュータ間を接続するために用いられる。しかし、IP アドレス交換に用いる VPN では、接続する 2 名の利用者は、見ず知らずの他人であり、相互に相手から攻撃される危険性にさらされる。本研究で用いた Tinc VPN は、PC を Layer 2 で接続するものであり、単純に用いれば LAN やホスト PC が危険にさらされる。本研究では、VPN のサーバにおいては、LAN へのアクセスを禁止し、インターネットにのみアクセス可能にする。そのために、Tinc VPN のサーバ側においては、Linux が持つソフトウェア的なスイッチング・ハブの機能(ブリッジ機能)とアドレス変換機能を用いて、クライアントからのパケットはインターネットしか送信されないようにした。さらに、VPN のクライアント側においても、コンテナ技術の１つ、Docker を用いて保護する機能を実現した。まず、VPN 接続相手から攻撃される可能性があるアプリケーションは、Docker コンテナにおいて実行する。そのコンテナでは、Web ブラウザ等のアプリケーションを実行するが、VPN 経由でインターネットしかアクセスできないようにする。すなわち、LAN やローカル・ホストへのアクセスを禁止する。これにより、攻撃を受けたとしても、被害がコンテナ内に限定される。

＜引用文献＞

① Daiyuu Nobori and Yasushi Shinjo: "VPN Gate: A Volunteer-Organized Public VPN Relay System with Blocking Resistance for Bypassing Government Censorship Firewalls", 11th USENIX Symposium on Networked Systems Design and Implementation, 2014, pp.229-241.

５．主な発表論文等

〔雑誌論文〕（計８件）

① 河野 匠, 新城 靖, 佐藤 聡, 中井 央: ″DOM 木の同期を支援する分散型 Web ブラウザの提案″, 情報処理学会第 30 回コンピュータシステム・シンポジウム(ComSys2018) ポスターセッション, 2 ページ (2018 年 11 月 29 日-30 日). 査読無.
http://www.ipsj.or.jp/sig/os/index.php?plugin=attach&refer=ComSys2018%20%A5%DD%A5%B9%A5%BF%A1%BC%A5%BB%A5%C3%A5%B7%A5%E7%A5%F3&openfile=ComSys2018_paper_16.pdf

② Meng Li and Yasushi Shinjo: ″Grouper: A Framework for Developing Mobile Applications using a Secret Sharing Scheme and Untrusted Servers″, In Proceedings of the 2017 VI International Conference on Network, Communication and Computing

(ICNCC 2017), pp.125-134 (December 14-16, 2017). 査読有.
https://doi.org/10.1145/3171592.3171628

③ 田中 創樹, 新城 靖: "ノード間通信が可能なボランティアコンピューティング", 情報処理学会第29回コンピュータシステム・シンポジウム(ComSys2017), pp.96-104 (2017年12月5日-7日). 査読無. http://id.nii.ac.jp/1001/00184599/

④ Yasushi Shinjo, Sota Naito, Xiao Kunyao, Akira Sato: "ABnews: A fast private social messaging system using untrusted storage and attribute-based encryption", IEEE 15th Annual Conference on Privacy, Security and Trust (PST 2017), 10 pages (August 28-30, 2017, Calgary, Canada). 査読有.
https://doi.org/10.1109/PST.2017.00045

⑤ Meng Li and Yasushi Shinjo: "A Proposal for Implementing Mobile Applications Using Untrusted Servers", 情報処理学会第28回コンピュータシステム・シンポジウム (ComSys2016) ポスターセッション, 2 pages (2016年11月28日).
http://www.ipsj.or.jp/sig/os/index.php?plugin=attach&refer=ComSys2016%20%A5%DD%A5%B9%A5%BF%A1%BC%A5%BB%A5%C3%A5%B7%A5%E7%A5%F3&openfile=ComSys_2016_paper_31.pdf

⑥ 田中 正規, 新城 靖, 佐藤 聡, 中井 央: " 自律的なソーシャルVPNの設計と実装", 情報処理学会第28回コンピュータシステム・シンポジウム(ComSys2016), pp.137-146 (2016年11月28日-30日). 査読無. http://id.nii.ac.jp/1001/00176021/

⑦ Yasushi Shinjo, Naoki Kainuma, Daiyuu Nobori, and Akira Sato: "Magic Mantle using Social VPNs against Centralized Social Networking Services", IEEE 14th Annual Conference on Privacy, Security and Trust (PST 2016), pp.341-348 (December 12-14, 2016, Auckland, New Zealand). 査読有. https://doi.org/10.1109/PST.2016.7906984

⑧ Lai Rongchang and Yasushi Shinjo: "Sweets: A Decentralized Social Networking Service Application Using Data Synchronization on Mobile Devices", The 12th International Conference on Collaborative Computing: Networking, Applications and Worksharing (CollaborateCom 2016), pp.188-198, (November 12-13, 2016, Beijing, People's Republic of China). 査読有. https://doi.org/10.1007/978-3-319-59288-6_17

〔その他〕
ホームページ http://www.softlab.cs.tsukuba.ac.jp/

６．研究組織

(1)研究代表者
研究代表者氏名：新城　靖
ローマ字氏名：SHINJO, Yasushi
所属研究機関名：筑波大学
部局名：システム情報系
職名：准教授
研究者番号（8桁）：00253948

(2)研究分担者
研究分担者氏名：佐藤　聡
ローマ字氏名：SATO, Akira
所属研究機関名：筑波大学
部局名：システム情報系
職名：准教授
研究者番号（8桁）：90285429