UMA ANÁLISE DE NAVEGAÇÃO NO MODO PRIVATIVO DO GOOGLE CHROME MOBILE

Resumo: Com as revelações sobre a invasão de privacidade ocorridas em 2013, houve um considerável aumento da busca por maior segurança na sociedade, fato que afetou a indústria de desenvolvimento tecnológico. Um exemplo seria o do navegador Firefox, que, na sua versão 43, adicionou ao modo de navegação privada o bloqueio de rastreadores de terceiros baseado na lista do Disconnect, uma empresa que atua no contexto de segurança e privacidade online.

A primeira ocorrência da implementação da funcionalidade de Modo Privativo (Privacy Mode) foi registrada em 2005, a qual tem como objetivo principal impedir o armazenamento local de dados de navegação que poderiam ser acessados posteriormente.

Na atualidade, a fração de usuários que acessam a web via navegador móvel aponta crescimento significativo – que acompanha, proporcionalmente, preocupações com relação à segurança e privacidade dos dados envolvidos em sua navegação. A maior porção desses usuários utilizam o navegador Google Chrome Mobile (número que cresce devido ao Google gradativamente tornar o Chrome o navegador padrão do Android a partir da versão 4.0) e entendem, de maneira geral, o Modo Privativo como uma ferramenta de incremento de segurança.

O presente trabalho apresenta uma análise do comportamento do navegador Google Chrome Mobile utilizando o Modo Privativo (Incognito Mode) por meio de duas abordagens:

1) Análise de consistência entre o propósito original da criação do Modo Privativo, veiculado via marketing, e sua utilização prática.

2) Análise de segurança e privacidade da navegação.

Palavras-chave: privacidade, segurança, mobile, browser, google chrome

THIAGO NOBAYASHI*
LEONARDO KAZUHIKO KAWAZOE **

Un análisis de la navegación en Modo Privativo de Google Chrome Mobile

Resumen: Con las revelaciones sobre la invasión de privacidad ocurridas en 2013, ocurrió un considerable aumento de la busca por mas seguridad en la sociedad, hecho que afectó la industria de desarrollo tecnológico. Un ejemplo sería el de navegador firefox, en que, en su versión 43, adicionó al modo de navegación privada el bloqueo de rastreadores de terceros basado en la lista del Disconnect, una empresa que actúa en el contexto de seguridad y privacidad online. La primera ocurrencia de implementación da funcionalidad del Modo Privativo (Privacy Mode) fue registrada en 2005, la cual tiene como objetivo principal impedir el almacenamiento local de datos de navegación a los que podría accederse posteriormente.

En la actualidad, la fracción de usuarios que accede a la web a través de navegador móvil señala un crecimiento significativo - que acompaña, proporcionalmente, preocupaciones con la relación a la seguridad y privacidad de los datos involucrados en su navegación. La mayor parte de estos usuarios utilizan el navegador Google Chrome Mobile (número que crece debido a que el Google gradualmente torna el Chrome, el navegador padrón del Android a partir de la versión 4.0) y entienden, de manera general, el Modo Privativo como una herramienta de aumento de seguridad.

El Presente trabajo presenta un análisis del comportamiento del navegador Google Chrome Mobile utilizando el Modo Privativo (Incognito Mode) por medio de dos enfoques:

1) Análisis de la consistencia entre el propósito original de la creación del Modo Privativo, vinculado vía marketing, y su utilización práctica.

2) Análisis de seguridad y privacidad de navegación.

Palabras clave: privacidad, seguridad, móvil, navegador, google chrome.

A navigation analysis in Google Chrome Mobile Private Mode

Abstract: In consequence of the last revelations about the invasion of privacy in 2013 there was a considerable increase of the search for more security in society, which has been affecting the industry of technology development. An example is the Firefox web navigator, which in the version 43 added to its private navigation mode the block of third-party trackers based in the Disconnect list (Company engaged in the context of security and privacy).

The first occurrence of the implementation of the Private mode functionality was recorded in 2005, which aims to prevent the local storage of navigation data that could be accessed posteriorly.

Currently, the fraction of users who access the web via mobile browser points had significant growth accompanying proportionally concerns regarding the security and privacy of data involved in navigation. The major portion of these users use Google Chrome Mobile browser (number growing due to Google gradually make Chrome the default browser of Android from the version 4.0) and understand, in general, the Private Mode as a safety increment tool.

This work presents a Google Chrome Mobile browser behavior analysis using the Private Mode (Incognito Mode) through two approaches:

1) Consistency analysis between the original purpose of creation of the Private Mode, broadcasted via marketing, and its practical use.

2) Safety analysis and privacy of navigation.

Keywords: privacy, security, mobile, browser, google chrome.

INTRODUÇÃO

Como colocado por Wood e Wright (2015) 11 de setembro de 2001 se torna um gatilho para a vigilância, e uma boa oportunidade para as agências de vigilância se fortaleçam em cima de uma nova via massiva de dados, muito mais que os dados “freely given” fornecidos pelos usuários de redes sociais. Presenciamos vários estados atacando as características que fazem a internet um espaço criativo e livre, em nome de vários os tipos de riscos (terrorismo, crime de identidade,

crime de propriedade intelectual, pedofilia) , e restringir a internet se torna uma maneira para que as diversas agências de inteligência como a Agência Nacional de Segurança dos EUA (NSA) a monitorem de maneira mais fácil.

Nesse contexto em 2013 Edward Snowden, um administrador de sistemas, trabalhando para a NSA, revela para o mundo documentos disponibilizados através dos jornais the*Guardian* , the *New York Times* , *Der Spiegel* e *Washington Post* , e com isso nasce um novo entendimento de várias dimensões do ciberespaço, Bajaj (2014). Revelando sobre a vigilância global feita pela NSA, Snowden muda toda a conjuntura mundial em volta do controle de informações e da privacidade de governos, empresas privadas e da sociedade civil, criando um debate mundial em torno da garantia dos direitos civis, privacidade e liberdade na rede.

Edward Snowden também revela informações sobre como as grandes empresas de tecnologia norte americanas sabiam sobre o esquema de vigilância e participavam de maneira ativa, umas destas empresas sendo o*Google* . No artigo "Google is not what it not what it seems" publicado no *WeakiLeaks* por Assange (2014), este compilando várias denúncias em relação a atuação do *Google* junto ao governo dos EUA. Sabendo que a privacidade das bilhões de pessoas que acessam a internet já estava comprometida por um acordo entre vários estados ao redor do mundo agora temos a maior companhia do mundo (Hern, 2016) atuando também no esquema global de vigilância.

Além das problemáticas de se usar produtos*Google* , e da vigilância realizada por órgãos de vigilância e de estados, alguns dos interesses pelos quais a sociedade civil opta usar o modo privativo dos navegadores como solução para problemas de privacidade acabam por não condizer com as funcionalidades divulgadas pelas empresas responsáveis pelos navegadores, muito menos condiz com a conjuntura global de vigilância do ciberespaço.

Nesse artigo vamos analisar especificamente o modo privativo do navegador Google Chrome por ser navegador mais utilizado no mundo atualmente, inclusive no ambiente mobile, que vem crescendo cada vez mais tanto em número absoluto de usuários, como também em porcentagem de usuários que acessa a internet exclusivamente via mobile segundo dados e análises da plataforma (http://www.internetlivestats.com/).

A Empresa lança sua navegação anônima (Incognito Mode) em 2008, vem com o objetivo de cobrir uma gama de usuários que buscam por alguns tipos de privacidade em níveis diferentes. Combinado com o aumento dos acessos à internet exclusivamente via mobile, temos alguns pontos para analisar:

- O modo privativo do Google Chrome Mobile cumpre as funcionalidades divulgadas pelo empresa?
- Seguindo os motivos citados por Aggarwal, Bursztein, Jackson & Boneh (2010) para qual motivos as pessoas usam o modo privativo, o navegador contempla essas funcionalidades?

ANÁLISE DE SEGURANÇA

Contexto

A primeira ocorrência da implementação da funcionalidade de modo privativo (privacy mode) foi registrada em 2005, no navegador Safari, segundo Satvat, Forshaw, Hao & Toreini (2014). Quando ativa, impede que rastros de navegação, tais como histórico, cookies e arquivos temporários sejam armazenados no dispositivo local, diferentemente da mecânica usual. Esta – até então recente – mudança foi propagada para os demais, e, hoje, todos os principais navegadores possuem alguma função semelhante (Google Chrome, Mozilla Firefox, Internet Explorer).

O modo privativo no Google Chrome (para ambas as versões desktop e mobile) é implementado pela funcionalidade de modo incógnito (incognito mode). De acordo com suas especificações, os históricos de visitas a websites e de download não são armazenados nos dispositivos dos usuários (informações básicas como endereço de URL, páginas em cache ou endereços de websites visitados), qualquer cookie criado durante uma sessão privativa é deletado quando todas as sessões privativas são encerradas, permissões concedidas durante uma sessão anônima não são salvas ("Explore the Chrome Browser," n.d.), e traços de cache nem de armazenamento local são deixados ("Google Chrome," n.d.). Estes comportamentos são reiterados em seu documento de políticas de privacidade ("Google Chrome Privacy Notice," 2016).

Porém, é importante notar algumas ressalvas:

- Apesar do modo incógnito prevenir com que as atividades de visita não sejam armazenadas, o tráfego da rede pode ser monitorada por diversos agentes, tais como o administrador da rede ou o provedor do serviço de Internet;
  O navegador possui acesso às informações do perfil de usuário (senhas, sugestões baseadas em histórico de navegação), e estas são carregadas, mesmo durante uma sessão privativa;
- Páginas marcadas no modo incógnito serão salvas;
- A lista de downloads também não será salva, mas os arquivos descarregados serão salvos no diretório destinado a downloads da máquina do usuário.

Os pontos citados acima não são responsabilidades delegadas à segurança e privacidade dos navegadores – por não fazer parte de seu escopo de controle – , mas são características que proporcionam indiretamente brechas acidentais à integridade do usuário. O forte discurso de venda pode ser um fator agravante neste contexto, considerando que este tipo de tecnologia é universalmente difundido (não limitando seu acesso a especialistas) e a interpretação dos termos segurança e privacidade – enunciados pelo modo privativo – são subjetivos ao público de incidência.

Pode-se entender por privacidade neste contexto a definição colocada por Vianna (2009), em que se coloca a privacidade como um direito composto por três outros direitos, sendo eles:

- Direito de não ser monitorado, entendido como direito de não ser visto, ouvido, etc.;
- Direito de não ser registrado, entendido como direito de não ter imagens gravadas, conversas gravadas, etc.;
- Direito de não ser reconhecido, entendido como direito de não ter imagens e conversas anteriormente gravadas publicadas na Internet em outros meios de comunicação.

A análise será feita fundamentada pelos parâmetros definidos pela navegação privativa: o modo incógnito, enquanto sistema computacional, deve ser avaliado em termos de segurança de acordo com os objetivos assumidos pela ferramenta e como estes são cumpridos. A falha de execução de algum destes objetivos servirá de critério para definir este evento como uma violação do sistema e, portanto, da segurança.

Sendo assim, o tema do texto será discutido baseado nestas noções de segurança e privacidade.

PREMISSAS

De acordo com um estudo conduzido e publicado pelo grupo de Criptografia Aplicada da Universidade de Stanford (Aggarwal, Bursztein, Jackson & Boneh, 2010), a implementação do modo privativo nos navegadores possui fundamentalmente dois propósitos:

1. Impedir que rastros de navegação sejam deixados nos dispositivos dos usuários (em outras palavras, proteger contra ataques locais). Em linhas diretas, impedir o acesso ao conteúdo de navegação, posteriormente ao término da sessão de um usuário. Não salvar o histórico de*websites* visitados e de *downloads* são medidas que contribuem para o anonimato desejado atingir por este objetivo;
2. Permitir que a identidade do usuário seja preservada enquanto navega e acessa o conteúdo da rede (proteger os usuários contra ataques na*web*). Portanto:

2.1. Impedir com que seja possível criar conexão entre o mesmo usuário ao utilizar perfis públicos e privativos;

2.2. Impedir com que seja possível criar conexão entre o mesmo usuário em diferentes sessões de perfis privativos;

2.3. E é desejável que não seja possível identificar quando um usuário está no modo privativo.

Deletar os*cookies* após todas as sessões anônimas serem encerradas, e não deixar *cookies* obtidos em navegação padrão disponíveis à navegação privativa podem ser encarados como uma tentativa de prevenção a este objetivo. Porém, não é suficiente.

Segundo Mayer (2009), uma série de características podem ser extraídas de um navegador utilizando apenas objetos JavaScript padrões, tais como nível de*zoom* , geolocalização, fontes instaladas, dados da rede, *plugins* instalados e resolução. Estas informações servem para corroborar a demonstração, feita pela Electronic Frontier Foundation (Eckersley, 2010), de que é possível utilizar as diversas características extraíveis do navegador para se gerar *fingerprints*, e, portanto, eliminar as chances de atingir os objetivos 2.1 e 2.2.

De acordo com Boneh*et al,* é possível classificar mudanças de estados persistentes em quatro categorias:

I. Mudanças iniciadas por*websites* , que não requerem interação com o usuário, tal como adicionar dados ao cache do navegador;

II. Mudanças iniciadas por*websites* , que requerem interação com o usuário, tal como adicionar uma senha à base de dados de senhas;

III. Mudanças iniciadas por usuários, tais como adicionar um*website* aos favoritos ou o *download* de um arquivo;

IV. Mudanças não específicas do usuário, tal como a instalação de*patches* .

ANÁLISE

Os navegadores tentam apagar as mudanças de estado do tipo I ao finalizar todas as sessões privativas. Caso isso não seja possível, pode-se considerar que há uma violação da navegação privativa.

Como os objetivos em 2 podem ser considerados como inalcançáveis, o que resta é tentar tratar de forma eficaz os objetivos em 1, que também não são triviais. Outro aspecto descrito por Aggarwal, Bursztein, Jackson & Boneh (2010) é de que ataques locais possuem inúmeras fontes, e um conjunto específico deles está relacionado ao sistema operacional (SO). Um destes problemas é o de que o navegador realiza a resolução de DNS ao acessar um dado*website* , e o SO frequentemente faz o cache desta resolução, deixando rastros da lista de acessos feitos. Uma solução para isto seria a limpeza do cache de DNS após o término das sessões privativas – o que aparentemente não é feito. Outro problema está relacionado ao *swap* de memória do SO, que pode acessar partições de memória e deixar rastros de atividades do usuário, enquanto navega.

Outro fato interessante é de que quando o Google Chrome utiliza a memória cache da GPU, esta não é deletada após o término de uma sessão (seja ela privativa ou não). Sendo assim, existem brechas que podem ser exploradas para que seja possível recuperar imagens renderizadas durante uma sessão anônima, utilizando o cache da GPU. Aparentemente este*bug* foi reportado, mas ignorado por não fazer parte do design do navegador.

Por fim, um simples experimento foi executado, utilizando a metodologia a seguir:

- Uma cópia da aplicação Google Chrome Mobile versão 54.0.2840.68 foi baixada e instalada num dispositivo móvel, rodando o Android sob a versão 4.1.2;
- A aplicação foi executada e ativado o modo incógnito;
- Foi verificado o*timestamp* dos diretórios pertencidos pela aplicação, em */data/data/* ;
- Foi executado um pedido HTTPS para um*website* ;
- O*timestamp* dos diretórios pertencidos pela aplicação, em */data/data/* , foi verificado novamente.

Pôde-se notar, sem grandes análises, que o*timestamp* de alguns diretórios foram alterados – talvez pelos dados de navegação terem sido deletados –, ou seja, é possível determinar quando um usuário utiliza a aplicação, em modo incógnito ou não.

MARKETING

A funcionalidade de modo incógnito é ofertada para ocasiões em que não se é desejado registrar os*websites* visitados e *downloads* feitos. De acordo com o estudo conduzido pela Universidade de Stanford (Aggarwal, Bursztein, Jackson & Boneh, 2010), é sugerido que o uso primário do modo privativo esteja relacionado ao acesso de conteúdo adulto – que pode ser resumido a atividades de caráter íntimo. Sendo assim, pode-se identificar que há compatibilidade entre o modo em que se é vendida a funcionalidade e como esta é utilizada de modo prático, majoritariamente.

CONSIDERAÇÕES FINAIS

O caso analisado é singular no sentido de que nem sempre a coerência entre como se é vendido e utilizado na prática, o produto, é positiva. A finalidade descrita por ambos empresa e usuários acabam por ser semelhantes, mas seus objetivos claramente vão em direções opostas, fato que potencialmente se estende a uma problemática interdisciplinar: o crescente número de usuários de navegadores móveis, em busca de privacidade acabam por cair em sua total contradição, em relação ao comportamento real do sistema enquanto máquina computacional, por exemplo.

A falsa sensação de privacidade e anonimato no ambiente virtual pode acabar por gerar consequências irreversíveis para usuários e para pessoas que, de alguma maneira, se relacionam com eles. Este artigo tenta expor que a análise dessas informações continuamente registradas e monitoradas em larga escala ou em nível pessoal geram impacto e controle sem precedentes na sociedade e em nossas vidas, sem ao menos que tenhamos noção, na maioria das vezes, de como isso nos afeta a nível pessoal e como indivíduo e em relação a conjuntura política internacional em torno da vigilância.

Percebe-se essa contradição tanto na falta de conhecimento ou abstração do quão problemática vigilância é nos âmbitos pessoais, sociais e políticos quanto no conhecimento técnico de como essas ferramentas funcionam. Isso acaba por gerar nesse grande espectro de usuários a falsa sensação de anonimato e privacidade quando estão no ambiente virtual, em relação a casos de uso diários como simples compras, pesquisas e acesso a conteúdo

NOTAS

* Estudante de Graduação no Bacharelado em Sistemas de Informação na Escola de Artes Ciências e Humanidades da Universidade de São Paulo (EACH - USP). thiago.nobayashi@usp.br

** Estudante de Graduação no Bacharelado em Sistemas de Informação na Escola de Artes Ciências e Humanidades da Universidade de São Paulo (EACH - USP). leonardo.kawazoe@usp.br

REFERÊNCIAS

Vianna, T. L. (2007).*Transparência pública, opacidade privada* (Doctoral dissertation, Universidade Federal do Paraná Curitiba).

Mayer, J. R. (2009). Any person... a pamphleteer": Internet Anonymity in the Age of Web 2.0.*Undergraduate Senior Thesis, Princeton University*.

Eckersley, P. (2010). A primer on information theory and privacy.*Electronic Frontier Foundation* .

Aggarwal, G., Bursztein, E., Jackson, C., & Boneh, D. (2010, August). An Analysis of Private Browsing Modes in Modern Browsers. In*USENIX Security Symposium* (pp. 79-94).

Bajaj, K. (2014). Cyberspace: Post-Snowden.*Strategic Analysis* , *38* (4), 582-587.

Google Is Not What It Seems. (2014). Recuperado dehttps://wikileaks.org/google-is-not-what-it-seems/

Satvat, K., Forshaw, M., Hao, F., & Toreini, E. (2014). On the privacy of private browsing–a forensic approach. In*Data Privacy Management and Autonomous Spontaneous Security* (pp. 380-389). Springer Berlin Heidelberg.

Wood, D. M., & Wright, S. (2015). Before and After Snowden.*Surveillance and Society* , *13* (2), 132-138.

Browse in private with Incognito mode. (n.d.). Recuperado dehttps://support.google.com/chrome/answer/95464?hl=en&p=cpn_incognito

Hern, A. (2016, 2 de fevereiro). How alphabet became the biggest company in the world.*The Guardian* . Recuperado de https://www.theguardian.com/technology/2016/feb/01/how-alphabet-made-google-biggest-company-in-the-world

Explore the Chrome Browser. (n.d.). Recuperado dehttps://www.google.com.br/chrome/browser/features.html

Google Chrome Privacy Notice. (2016, August 30). Recuperado dehttps://www.google.com/chrome/browser/privacy/

Google Chrome. (n.d.). Recuperado dehttps://www.google.com.br/mobile/chrome/