Universidade Federal de Pernambuco
Centro de Informática

Graduação em Engenharia da Computação

Métodos governamentais de censura e vigilância na Internet

Rodolfo Cesar de Avelar Ferraz

Trabalho de Graduação

Recife
2 de outubro de 2013

Universidade Federal de Pernambuco
Centro de Informática

Rodolfo Cesar de Avelar Ferraz

Métodos governamentais de censura e vigilância na Internet

Trabalho apresentado ao Programa de Graduação em Engenharia da Computação do Centro de Informática da Universidade Federal de Pernambuco como requisito parcial para obtenção do grau de Bacharel em Engenharia da Computação.

Orientador: *Prof. Ruy José Guerra Barretto de Queiroz*

Recife
2 de outubro de 2013

À minha família, aos meus amigos e aos meus professores, por terem me ajudado na minha formação, cada um à sua maneira. Ao universo, por ter me dado a chance de conhecê-los.

This concern with the basic condition of freedom – the absence of physical constraint – is unquestionably necessary, but is not all that is necessary. It is perfectly possible for a man to be out of prison, and yet not free – to be under no physical constraint and yet to be a psychological captive, compelled to think, feel and act as the representatives of the national State, or of some private interest within the nation, want him to think, feel and act. There will never be such a thing as a writ of habeas mentem; for no sheriff or jailer can bring an illegally imprisoned mind into court, and no person whose mind had been made captive by the methods outlined in earlier articles would be in a position to complain of his captivity. The nature of psychological compulsion is such that those who act under constraint remain under the impression that they are acting on their own initiative. The victim of mind-manipulation does not know that he is a victim. To him, the walls of his prison are invisible, and he believes himself to be free. That he is not free is apparent only to other people.

—ALDOUS HUXLEY (Brave New World Revisited, 1958)

Resumo

Desde a popularização das redes sociais é perceptível que a população vem se tornando mais atuante politicamente. Através de Facebook e Twitter, vemos mobilizações feitas por e a favor da população, coisa que não acontecia antes desta popularização. A inércia já é coisa do passado, e não se depende mais de meios de comunicação em massa controlados, como jornais, rádio e televisão, que omitem ou veiculam notícias com vieses de acordo com seus interesses. Quem cria as notícias são a própria população, cada um com sua perspectiva, e desta forma, conseguimos nos aproximar da realidade, e não mais uma realidade maquiada, como nos era apresentada pelos meios televisivos, que esperançosamente venham a se tornar obsoletos.

Este novo grau de comunicação deve ser sempre garantido a todas as nações e todas as classes sociais, independente das vontades governamentais, a fim de garantir a evolução social. Logo, deve-se estudar formas de projetar a rede mundial a fim de tornar impossível quaisquer censuras ou formas de coibir a comunicação entre as pessoas.

Este trabalho tenta discriminar as formas mais comuns de censurar e vigiar cidadãos, inclusive praticados contemporaneamente, assim como os métodos que estes mesmos cidadãos podem utilizar para contornar este abuso contra os direito humanos, praticado pelos seus governantes.

Teste cite [Ada06] e ref [DMS04].

Palavras-chave: censura, vigilância, segurança, privacidade, anonimidade, internet, tecnologia e sociedade, direitos humanos

Abstract

Lorem ipsum dolor sit amet, consectetuer adipiscing elit. Ut purus elit, vestibulum ut, placerat ac, adipiscing vitae, felis. Curabitur dictum gravida mauris. Nam arcu libero, nonummy eget, consectetuer id, vulputate a, magna. Donec vehicula augue eu neque. Pellentesque habitant morbi tristique senectus et netus et malesuada fames ac turpis egestas. Mauris ut leo. Cras viverra metus rhoncus sem. Nulla et lectus vestibulum urna fringilla ultrices. Phasellus eu tellus sit amet tortor gravida placerat. Integer sapien est, iaculis in, pretium quis, viverra ac, nunc. Praesent eget sem vel leo ultrices bibendum. Aenean faucibus. Morbi dolor nulla, malesuada eu, pulvinar at, mollis ac, nulla. Curabitur auctor semper nulla. Donec varius orci eget risus. Duis nibh mi, congue eu, accumsan eleifend, sagittis quis, diam. Duis eget orci sit amet orci dignissim rutrum.

Keywords: <DIGITE AS PALAVRAS-CHAVE AQUI>

Sumário

CAPÍTULO 1

Introdução

1.1 Motivação e Contextualização

1.1.1 A influência da Internet na sociedade

Pablo Capilé[1] expressa bem a mudança da dinâmica informacional no Brasil e no mundo: "Antes existia apenas mídia de massa, agora também temos massa de mídia". Antes da Internet, os fatos eram filtrados e apresentados por grupos restritos, para uma grande massa de ouvintes e leitores. Agora, aqueles que agiam passivamente, apenas lendo e ouvindo podem ser geradores de conteúdo, indo para a rua com seu smartphone e mostrando sua visão dos fatos.

A Figura 1.1 mostra um exemplo de streaming de vídeo, feito pela

1.1.1.1 A Primavera Árabe

Lorem ipsum dolor sit amet, consectetuer adipiscing elit. Ut purus elit, vestibulum ut, placerat ac, adipiscing vitae, felis. Curabitur dictum gravida mauris. Nam arcu libero, nonummy eget, consectetuer id, vulputate a, magna. Donec vehicula augue eu neque. Pellentesque habitant morbi tristique senectus et netus et malesuada fames ac turpis egestas. Mauris ut leo. Cras viverra metus rhoncus sem. Nulla et lectus vestibulum urna fringilla ultrices. Phasellus eu tellus sit amet tortor gravida placerat. Integer sapien est, iaculis in, pretium quis, viverra ac, nunc. Praesent eget sem vel leo ultrices bibendum. Aenean faucibus. Morbi dolor nulla, malesuada eu, pulvinar at, mollis ac, nulla. Curabitur auctor semper nulla. Donec varius orci eget risus. Duis nibh mi, congue eu, accumsan eleifend, sagittis quis, diam. Duis eget orci sit amet orci dignissim rutrum.

1.1.2 O perigo da ignorância sobre o funcionamento da Internet

A Internet traz benefícios a todos, no entanto, praticamente apenas aqueles ligados a área de Tecnologia da Informação têm conhecimento sobre seu funcionamento. Quando se dirige um

[1] Pablo Capilé é uma das lideranças do movimento Fora do Eixo e um dos idealizadores do grupo Mídia NINJA. O Fora do Eixo é uma rede de pessoas, criada inicialmente para possibilitar a circulação de artistas independentes, de fora do eixo Rio-São Paulo. Com o tempo, o movimento cresceu, e a partir dele outras iniciativas surgiram. Uma delas foi o Mídia NINJA (Narrativas Independentes, Jornalismo e Ação), declarada como uma alternativa à imprensa tradicional. Sua característica marcante é transmitir acontecimentos ao vivo, utilizando streaming via smartphones, muitas vezes apresentando opinião e apoio explícito a algumas causas, diferentemente da mídia tradicional que tenta transmitir uma imparcialidade, embora muitas vezes tente apresentar a informação de forma que suporte seus interesses. A transmissão pode ser feita por mais de uma pessoa simultaneamente, podendo apresentar diferentes pontos de vista sobre um mesmo tema.

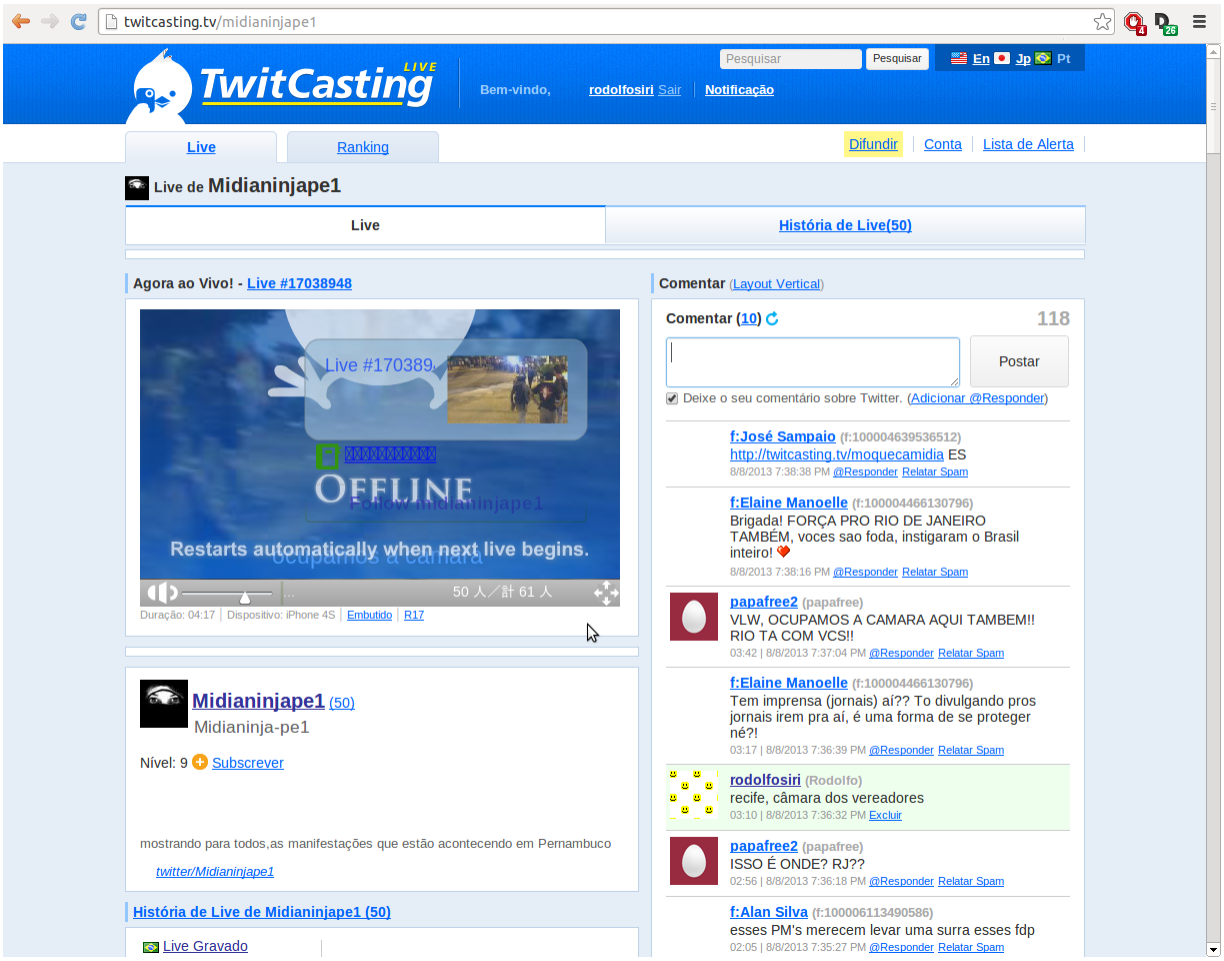

Figura 1.1 Através de um aplicativo para celular e conexão 3G, centenas de pessoas puderam assistir à ocupação da Câmara de Vereadores do Recife, durante reivindicação de planos para passe livre de ônibus entre outras. O celular do "ninja"como alguns chamam os jornalistas que transmitem nesses moldes perdia o sinal ao se aproximar muito da Câmara. Por isso, muitas vezes a transmissão era interrompida. No momento, a Mídia NINJA era a única fonte de informação sobre a ocupação da câmara. As mídias tradicionais, com um processo mais burocrático de gerar notícia, acabou

automóvel, não é necessário que o motorista domine o funcionamento interno do motor do veículo. O mesmo acontece com a Internet, pois não precisamos conhecer como funciona para utilizá-la, no entanto através dela podemos nos expressar livremente e ter acesso a informações que não seriam alcançáveis através de outro meio. Ou seja, a Internet é uma ferramenta que nos permite praticar diversos direitos fundamentais e qualquer mudança na forma como ela funciona pode impactar na prática desses direitos.

Por este motivo, é importante que a sociedade tenha um mínimo de conhecimento sobre o funcionamento desta ferramenta, e assim poder cobrar que ela esteja funcionando em favor dos seus direitos.

1.2 Objetivos

Este trabalho tem por objetivo explicar o funcionamento interno da Internet, num nível técnico acessível para leigos em computação e na profundidade necessária para entender como ela pode ser desvirtuada para ferir os seus direitos em vez de favorecê-los. Com este conhecimento em mãos, serão apresentados ao leitor as maneiras que diferentes governos utilizaram para controlar as informações acessíveis aos cidadãos, assim como os meios utilizados pelos cidadãos para contornar estes bloqueios. Ao fim do trabalho, o leitor deve estar ciente de que os benefícios trazidos pela Internet estão em constante ameaça, e que somente com a vigilância do povo sobre o governo e companhias de telecomunicação, poderemos ter a rede ao nosso favor.

1.3 Estrutura do trabalho

Lorem ipsum dolor sit amet, consectetuer adipiscing elit. Ut purus elit, vestibulum ut, placerat ac, adipiscing vitae, felis. Curabitur dictum gravida mauris. Nam arcu libero, nonummy eget, consectetuer id, vulputate a, magna. Donec vehicula augue eu neque. Pellentesque habitant morbi tristique senectus et netus et malesuada fames ac turpis egestas. Mauris ut leo. Cras viverra metus rhoncus sem. Nulla et lectus vestibulum urna fringilla ultrices. Phasellus eu tellus sit amet tortor gravida placerat. Integer sapien est, iaculis in, pretium quis, viverra ac, nunc. Praesent eget sem vel leo ultrices bibendum. Aenean faucibus. Morbi dolor nulla, malesuada eu, pulvinar at, mollis ac, nulla. Curabitur auctor semper nulla. Donec varius orci eget risus. Duis nibh mi, congue eu, accumsan eleifend, sagittis quis, diam. Duis eget orci sit amet orci dignissim rutrum.

CAPÍTULO 2

Fundamentos do funcionamento e infraestrutura da Internet

Any sufficiently advanced technology is indistinguishable from magic.
—ARTHUR C. CLARKE (Profiles Of The Future: An Inquiry into the Limits of the Possible, 1958)

Neste capítulo, será explicado de forma simplificada o funcionamento da rede que nos conecta a bilhões de outras pessoas todos os dias. Primeiro, será apresentada uma analogia com um serviço postal, para explicar como os dados são transmitidos pela rede, e as pequenas diferenças para um correio normal, que a tornam um meio de comunicação facilmente susceptível a vigilância e censura. Em seguida, serão apresentadas algumas definições necessárias para o entendimento do trabalho.

2.1 Analogia com serviço postal

A Internet funciona como o serviço de um correio. Cada encomenda possui um certo conteúdo e deve apresentar uma etiqueta contendo o endereço do remetente e o endereço destino. Antes de chegar ao destino final, os pacotes da Internet precisam passar por diversas agências e centros de distribuição. Neste correio, no entanto, o conteúdo das encomendas não é protegido. Qualquer elemento que participe da entrega pode ver o conteúdo, armazenar cópias, e o mesmo pode ser feito com a etiqueta contendo os endereços. Na verdade, muitos governos exigem que os responsáveis pelo trânsito destas "encomendas"copiem e armazenem esses dados por um tempo mínimo, para possíveis investigações policiais futuras.

Qualquer ponto que participe do reencaminhamento de pacotes, portanto, pode ser utilizado como elemento atuador de uma política de censura e vigilância. Para censurar, basta descartar pacotes que possuam conteúdo considerado inapropriado. Ou então, apenas a partir das informações da etiqueta, pode-se descartar mensagens remetidas por endereços específicos, ou endereçadas a tais destinos. Já a vigilância pode ser praticada com a simples gravação dos da-

dos, instalando uma espécie de gravador em um ponto de convergência de mensagens (centros de recebimento e reenvio).

2.2 O uso da criptografia na Internet

Infelizmente não são apenas as entidades envolvidas no tráfego dos dados que têm a chance de visualizar todo o conteúdo transmitido na rede. Os "piratas de computador", com toda sua expertise em computação e segurança, sem muita dificuldade encontram brechas de segurança e conseguem interceptar esses pacotes sem serem notados. Esses piratas podem ser criminosos, tentando auferir lucro a partir de informações como dados do cartão de crédito, ou podem ser espiões contratados para obter informações sigilosas de indivíduos, empresas ou governos. Para contornar esse problema, foram desenvolvidas soluções que têm como objetivo tornar a mensagem ilegível para leitores não autorizados. Apenas o destinatário é capaz de tornar a mensagem legível. Essas soluções se baseiam nos conceitos da criptografia, que existem há milênios, desde que o ser humano sentiu a necessidade de ocultar mensagens a indivíduos indesejados.

2.3 Pacotes IP

Outra diferença para um correio normal é que os carteiros, ou veículos que levam as encomendas, só são capazes de levar pacotes bem pequenos. Então, quase sempre o conteúdo a ser enviado é dividido em pacotes menores e enviados separadamente. Ao chegar no destinatário, o conteúdo das frações da encomenda são reunidos, formando-se o dado enviado originalmente.

Para tornar possível a comunicação e o entendimento entre diversos tipos de dispositivos em uma mesma rede, foi necessário estabelecer certos padrões. Estes padrões compõem o chamado protocolo de comunicação IP (Internet Protocol) e determinam o formato das mensagens transmitidas. Essas mensagens são digitais, ou seja, são formadas apenas por números. Não há etiquetas físicas, nem caixas, como num correio real. Na Internet, o endereço remetente é um número, o endereço destino é outro, e o conteúdo a ser enviado são mais números. Estes números são enviados em sequência e não há espaços, nem divisórias entre eles. Portanto, é preciso que o emissor e receptor combinem que informação vem primeiro e qual o comprimento de cada uma. O protocolo IP define isso. A sigla IP também é utilizada para se referir ao endereço que identifica cada participante da rede IP (outro nome para a Internet). Como dito anteriormente, os endereços são formados apenas por números. O comprimento do endereço IP é 32 bits, ou 4 bytes e pode ser representado como 4 bytes separados por pontos. Como um byte pode guardar valores de 0 a 255, então os endereços IP variam de 0.0.0.0 a 255.255.255.255.

Tudo que é acessível via Internet precisa ter um endereço IP. O Facebook possui um, o Youtube possui outro, e você, para acessá-los, também precisa de um.

Os pacotes trocados via Internet podem transportar vários tipos de dados: o texto de um e-mail, um vídeo do *Youtube*, a senha da sua conta do *Facebook* depois de você clicar em "Entrar", ou seja, tudo que trafega na rede são transformados em zeros e uns e enviados através destes pacotes. Ao chegar no destino, estes zeros e uns são reconvertidos para o tipo de conteúdo

original, seja o texto de e-mail ou vídeo do Youtube.

Logo, quando enviamos um pacote a partir do nosso computador, este pacote acompanha nosso endereço IP, o endereço IP do destinatário e o dado que será recebido por ele. Todas estas informações são lidas por diversos dispositivos que são responsáveis por encaminhar nosso pacote até o destino. Estes dispositivos muitas vezes armazenam todos estes dados por longos períodos.

2.3.1 Como funcionam a Web e os servidores de nomes

Para acessar um Website, primeiro é enviado um pacote ao computador (também chamado de servidor) que contém a página procurada. O conteúdo deste pacote é um pedido, requisitando a página inicial. O Website então responde com outros pacotes, contendo a página, que ao chegar no computador do internauta, é exibida no navegador. Quando o usuário clica em algum link do site, uma nova requisição é enviada, que por sua vez é respondida novamente com outra página. A navegação na Web funciona basicamente desta forma: requisições dos usuários e respostas dos servidores Web, em forma de páginas.

No entanto, para o correio entregar os pedidos de página do usuário, ele precisa do endereço IP destino. Este endereço é formado apenas por alguns números. Não há nomes, nem ruas, nem cidades neste endereço.

Como ficaria difícil para os internautas decorar os números dos endereços IP de todos os seus Websites favoritos, foi criada uma espécie de agenda de endereços, compartilhada em todo o mundo, que contém URLs (*Universal Resource Location*) associados a endereços IP. Assim, em vez de decorarmos que o endereço do Google é 74.125.234.240, basta que decoremos sua URL: *www.google.com*. Quando digitamos uma URL no nosso navegador, ele fica encarregado de consultar essa agenda e transformar o nome *www.google.com* em um endereço IP, para poder mandar o pacote com esse endereço. Essa agenda é armazenada em servidores conhecidos como Servidor DNS (*Domain Name System*) ou Servidor de Nomes. Como é de se esperar, os Servidores DNS também possuem um endereço IP, e se o usuário desejar, pode configurar qual servidor DNS será utilizado. Todavia, não há necessidade de ficar trocando o Servidor DNS, visto que todos devem responder da mesma forma. A agenda de nomes e endereços deve ser idêntica para todos conectados na Web.

2.4 Conceitos básicos

Provedor de Acesso Serviços e Informações da Rede Internet (Internet Service Provider - ISP). Garante que um indivíduo tenha acesso a toda a Internet e, para o caso de provedores de conteúdo, garantir que outros usuários possam visualizar seus serviços disponibilizados na rede.

Autonomous Systems (ASs). Todo ISP possui uma rede e caso esta rede possa adotar suas próprias políticas de administração de rede e seja registrada na LACNIC, ele terá responsabilidade pela sua rede e passará a ser um AS (Autonomous System), com um ASN (Autonomous System Number) que o identificará.

Peering. Para um cliente de um AS poder acessar o conteúdo de um cliente de outro AS, é necessário que exista uma conexão entre estes AS. Uma conexão direta entre os ASs é chamada de peering.

Trânsito. Uma forma de um AS fornecer acesso a vários outros ASs para seus clientes, seria fazer Peering com todos os outros ASs. No entanto há mais de 10000 ASs independentes no mundo, então torna-se inviável que um AS se conecte diretamente a todos os outros.

Caso uma rede AS1 queira se conectar com outra rede AS2, não é necessário que crie um peering (conexão direta) entre elas. A rede AS1 pode negociar com uma terceira rede AS3, que já possui Peering com a AS2, e pedir para usar a rede AS3 para ganhar acesso a AS2. O uso de uma ou várias redes ASs para alcançar uma rede destino é chamada de trânsito.

Tier One peer. Poucos ASs no mundo tem acesso a toda a Internet, mas não pagam por "trânsito"a nenhum outro ISP. Eles fazem "peering"com todos os "tier one"e vendem trânsito para os outros ISPs (ASs menores).

Portanto, para ter acesso a toda a Internet, ou o seu ISP ou um de seus "up-stream provider"terá conexão com pelo menos um "tier one".

Peering privado e Ponto de Troca de Tráfego. Se você não for um Tier One, obrigatoriamente terá que pagar por trânsito a algum outro AS para ter acesso a toda a Internet. No entanto, se você possuir Peering com algum AS, você economiza, pois esta conexão não passa por nenhum atravessador e você não precisa pagar por ela, apenas o custo de manutenção do link. Portanto, peering é de interesse de qualquer AS, pequeno ou grande.

Peering pode ser feito um a um, via interconexão direta (peering privado) ou através de um ponto de troca de tráfego (PTT), um local com uma infraestrutura compartilhada, onde os ISPs se juntam para interconectar suas redes. No caso, cada ISP pagará pelo uso dessa infraestrutura, mas não estarão pagando por trânsito, uma vez que estão conectados diretamente aos ASs que participam deste PTT.

Idealmente, existe no máximo um PTT em uma metrópole.

Ponto de Troca de Tráfego (PTT) ou Internet Exchange Point (IXP). Infraestrutura necessária para a interconexão direta entre as redes (Autonomous Systems - ASSs).

2.4.1 Subseção a

Lorem ipsum dolor sit amet, consectetuer adipiscing elit. Ut purus elit, vestibulum ut, placerat ac, adipiscing vitae, felis. Curabitur dictum gravida mauris. Nam arcu libero, nonummy eget, consectetuer id, vulputate a, magna. Donec vehicula augue eu neque. Pellentesque habitant morbi tristique senectus et netus et malesuada fames ac turpis egestas. Mauris ut leo. Cras viverra metus rhoncus sem. Nulla et lectus vestibulum urna fringilla ultrices. Phasellus eu tellus sit amet tortor gravida placerat. Integer sapien est, iaculis in, pretium quis, viverra ac, nunc. Praesent eget sem vel leo ultrices bibendum. Aenean faucibus. Morbi dolor nulla, malesuada eu, pulvinar at, mollis ac, nulla. Curabitur auctor semper nulla. Donec varius orci eget risus. Duis nibh mi, congue eu, accumsan eleifend, sagittis quis, diam. Duis eget orci sit

amet orci dignissim rutrum.

2.4.1.1 Subsubseção I

Lorem ipsum dolor sit amet, consectetuer adipiscing elit. Ut purus elit, vestibulum ut, placerat ac, adipiscing vitae, felis. Curabitur dictum gravida mauris. Nam arcu libero, nonummy eget, consectetuer id, vulputate a, magna. Donec vehicula augue eu neque. Pellentesque habitant morbi tristique senectus et netus et malesuada fames ac turpis egestas. Mauris ut leo. Cras viverra metus rhoncus sem. Nulla et lectus vestibulum urna fringilla ultrices. Phasellus eu tellus sit amet tortor gravida placerat. Integer sapien est, iaculis in, pretium quis, viverra ac, nunc. Praesent eget sem vel leo ultrices bibendum. Aenean faucibus. Morbi dolor nulla, malesuada eu, pulvinar at, mollis ac, nulla. Curabitur auctor semper nulla. Donec varius orci eget risus. Duis nibh mi, congue eu, accumsan eleifend, sagittis quis, diam. Duis eget orci sit amet orci dignissim rutrum.

2.4.2 Subseção b

Lorem ipsum dolor sit amet, consectetuer adipiscing elit. Ut purus elit, vestibulum ut, placerat ac, adipiscing vitae, felis. Curabitur dictum gravida mauris. Nam arcu libero, nonummy eget, consectetuer id, vulputate a, magna. Donec vehicula augue eu neque. Pellentesque habitant morbi tristique senectus et netus et malesuada fames ac turpis egestas. Mauris ut leo. Cras viverra metus rhoncus sem. Nulla et lectus vestibulum urna fringilla ultrices. Phasellus eu tellus sit amet tortor gravida placerat. Integer sapien est, iaculis in, pretium quis, viverra ac, nunc. Praesent eget sem vel leo ultrices bibendum. Aenean faucibus. Morbi dolor nulla, malesuada eu, pulvinar at, mollis ac, nulla. Curabitur auctor semper nulla. Donec varius orci eget risus. Duis nibh mi, congue eu, accumsan eleifend, sagittis quis, diam. Duis eget orci sit amet orci dignissim rutrum.

CAPÍTULO 3

Censura na Internet

he who controls the past controls the future, and he who controls the present controls the past

—GEORGE ORWELL (Nineteen Eighty-Four, 1949)

A prensa de tipos móveis inventada por Johannes Gutenberg, no século XV, revolucionou a disseminação de informação no ocidente, quando a impressão de livros era muito trabalhosa e pouco eficiente. O fato de mais pessoas terem acesso a livros foi considerado essencial para o início do Renascimento, período em que a sociedade se transformou em cultura, economia, política, religião, marcando o fim da Idade Média e início da Idade Moderna.

É notável que mudanças no acesso e fluxo de informação causam impactos na sociedade. Impactos também acontecem quando surgem novos meios de comunicação. Os governos e entidades censoras precisam se adaptar às novas formas de comunicação. Na época em que a comunicação escrita e impressa era a única forma de guardar conhecimento, a censura era feita através do recolhimento de livros e posterior incineração. Ao surgirem a radiodifusão e televisão, o conteúdo a ser veiculado poderia ser censurado pela própria emissora, temendo sofrer penalidades. Em alguns casos, o conteúdo a ser veiculado precisava ser revisado antes por entidades do governo, como já aconteceu durante a ditadura militar brasileira.

Na Internet, não é mais tão claro quem difunde informação e quem consome. Logo, a censura torna-se mais complexa. Muitas vezes, graças à falta de conhecimento técnico e ao desespero, peca-se pelo excesso, censurando informações que seriam aceitas sem problemas.

Além disso, devido à dinamicidade e complexidade da rede, as formas de censurar são menos triviais do que costumava acontecer no passado. Este capítulo irá descrever que formas um governo pode utilizar para realizar censura na Internet.

3.1 Remoção de conteúdo

O método mais simples de censura não utiliza meios tecnológicos, mas sim meios jurídicos, ou algum tipo de influência sobre o provedor de conteúdo a ser censurado. Através desta

influência, o autor do conteúdo, ou o servidor que contém a página é obrigado a remover o material indesejado pelo governo, sob pena de sofrer consequências caso não o faça.

A depender do país em questão, esse tipo de censura pode ser mais ou menos comum. Em alguns países, a quantidade de tipos de conteúdo proibidos é grande, sendo difícil para o governo monitorar todos os sites, mesmo em casos que força humana não é problema, como na China. Neste caso, pode-se terceirizar a censura.

3.1.1 Terceirização da censura

Na China, os provedores de conteúdo precisam ter uma licença concedida pelo governo para funcionarem. Caso seja encontrado em suas páginas algum conteúdo proibido, o provedor é responsabilizado, podendo perder sua licença. Desta forma, devido ao risco que corre caso não o faça, o próprio provedor exerce a função de censor, que seria do governo.

3.1.2 Legitimidade da censura

Nem todo tipo de censura é ruim. Certos tipos de ideias, por exemplo, se propagadas, podem levar ao ódio e violência. No Brasil, por exemplo, é proibido a apologia ao Nazismo. Já em alguns países árabes, é proibida a veiculação de pornografia. Quando o conteúdo fere de alguma forma as leis de um país, em que a nação como um todo é prejudicada devido à disponibilidade de um certo conteúdo, pode ser considerado justa a remoção do mesmo.

No entanto, a lei dos países diferem, então muitas vezes o conteúdo – mesmo que gerado dentro do país onde ele não é permitido – pode estar hospedado em outro país com legislação diferente. Neste caso, tudo que o país pode fazer é recorrer a meios tecnológicos, bloqueando o acesso ao conteúdo externo.

3.2 Bloqueio de acesso a conteúdo

3.2.1 DNS Poisoning

Como explicado na seção 2.3.1 da página 7, os servidores DNS são responsáveis por transformar URLs como *www.facebook.com* no endereço IP correspondente. Dessa forma, o usuário não precisa decorar o IP dos seus sites favoritos, basta lembrar a URL e digitá-la no navegador.

Uma forma de dificultar o acesso de usuários a certos sites é alterar as tabelas dos servidores DNS utilizados em um dado país, colocando endereços IP inválidos para os sites a serem censurados. Assim, quando o usuário digitar o endereço *www.facebook.com* no seu navegador, a sua requisição irá para um IP diferente daquele que o Facebook utiliza, provavelmente um IP inválido, ou de alguma página do governo avisando que aquele site está bloqueado.

No entanto, este método não é muito eficaz. Para contorná-lo, bastaria trocar de servidor DNS, ou decorar o IP do Facebook e digitá-lo na barra de endereços do navegador. Por isso, os governos também bloqueiam pacotes originados ou destinados a certos endereços IP.

3.2.2 Bloqueio a IPs

Os roteadores que recebem e reencaminham pacotes, podem ser configurados para descartar pacotes com certos endereços como remetente ou destinatário. Desta forma, torna-se impossível enviar pacotes diretamente a estes servidores.

3.2.3 Filtragem de pacotes

Também é possível filtrar pacotes não apenas pelos endereços envolvidos, mas também pelo conteúdo da mensagem. Citar o Skype versão chinesa.

Lorem ipsum dolor sit amet, consectetuer adipiscing elit. Ut purus elit, vestibulum ut, placerat ac, adipiscing vitae, felis. Curabitur dictum gravida mauris. Nam arcu libero, nonummy eget, consectetuer id, vulputate a, magna. Donec vehicula augue eu neque. Pellentesque habitant morbi tristique senectus et netus et malesuada fames ac turpis egestas. Mauris ut leo. Cras viverra metus rhoncus sem. Nulla et lectus vestibulum urna fringilla ultrices. Phasellus eu tellus sit amet tortor gravida placerat. Integer sapien est, iaculis in, pretium quis, viverra ac, nunc. Praesent eget sem vel leo ultrices bibendum. Aenean faucibus. Morbi dolor nulla, malesuada eu, pulvinar at, mollis ac, nulla. Curabitur auctor semper nulla. Donec varius orci eget risus. Duis nibh mi, congue eu, accumsan eleifend, sagittis quis, diam. Duis eget orci sit amet orci dignissim rutrum.

3.3 Empresas que lucram com a censura e a vigilância

Muitas empresas sediadas no ocidente ganham dinheiro produzindo sistemas para empregar vigilância e censura em países como Síria, Arábia Saudita, Irã e outros.

Citar blue coat, Müller, ...

3.4 A relação entre vigilância e censura – Autocensura

Lorem ipsum dolor sit amet, consectetuer adipiscing elit. Ut purus elit, vestibulum ut, placerat ac, adipiscing vitae, felis. Curabitur dictum gravida mauris. Nam arcu libero, nonummy eget, consectetuer id, vulputate a, magna. Donec vehicula augue eu neque. Pellentesque habitant morbi tristique senectus et netus et malesuada fames ac turpis egestas. Mauris ut leo. Cras viverra metus rhoncus sem. Nulla et lectus vestibulum urna fringilla ultrices. Phasellus eu tellus sit amet tortor gravida placerat. Integer sapien est, iaculis in, pretium quis, viverra ac, nunc. Praesent eget sem vel leo ultrices bibendum. Aenean faucibus. Morbi dolor nulla, malesuada eu, pulvinar at, mollis ac, nulla. Curabitur auctor semper nulla. Donec varius orci eget risus. Duis nibh mi, congue eu, accumsan eleifend, sagittis quis, diam. Duis eget orci sit amet orci dignissim rutrum.

CAPÍTULO 4

Vigilância na Internet

A intrínseca falta de transparência das agências de inteligência governamentais, somada aos seus poderes de interceptar comunicações privadas, acabam implicando em ações possivelmente ilegais ou criminosas. Exemplos dessas ações podem ser escutas telefônicas sem autorização judicial ou a detenção e interrogatório de estrangeiros, sem respaldo legal. Essa "falha de caráter"desse tipo de entidade se estende também ao contexto dos bits e bytes, onde estão espalhadas informações de todos nós. Neste capítulo serão abordados os diferentes métodos que tais entidades podem utilizar para invadir a privacidade dos cidadãos – legitimamente ou não.

4.1 Transmissão involuntária dos dados

4.1.1 Infecção do computador

Esta estratégia é mais comumente utilizada por criminosos que desejam roubar senhas de banco, por exemplo. Mas há registros de governos utilizando desta técnica.

Explicar sobre Cavalo de Troia. É possível ficar escutando o que entra/sai do computador pela rede, para tentar encontrar algum tráfego suspeito, possivelmente gerado por um Cavalo de Troia.

Pode ser um instalador enviado por anexo em um e-mail, disfarçado de mensagem de alguém conhecido, ou de alguma entidade bancária ou do governo, por exemplo.

Uma forma mais sofisticada é controlar um servidor DNS para converter nomes em IPs falsos, redirecionando usuários para cópias de páginas de bancos com fins maliciosos. Já aconteceu no Brasil em 2009 (? - ver livro Black Code).

Além destes ainda há os Infection Proxies, que ...

http://www.scmagazineuk.com/spy-malware-buried-on-official-tibetan-website/article/307285/

4.1.2 Infection Proxies

Palestra "Bugged Planet"de Andy Müller fala sobre Infection Proxies.

4.2 Interceptação dos dados em trânsito

4.2.1 Interceptação total dos dados

Mesmo com a máquina limpa, o usuário pode ser vigiado à distância, apenas escutando o que o usuário transmite. Neste caso o usuário não tem como descobrir se está sendo vigiado. A interceptação pode ser feita em vários lugares: interceptação de sinal WiFi, ou instalação de escutas no ISP a quem você se conecta, ou em um IXP que o seu ISP utiliza, no host com quem você se comunica,

Como funciona uma "escuta"na Internet? Como o Wireshark funciona? (modo promíscuo - via ethernet e via wifi)

4.2.2 Descoberta dos seus destinatários

Não é possível encriptar o cabeçalho IP. É através dele que os roteadores sabem a quem sua mensagem deve ser entregue. Por isso, esta informação está disponível para várias entidades diferentes, a começar pelo seu ISP. Existem formas de dificultar este rastreamento, mas de modo geral, é possível descobrir os principais servidores com os quais você se comunica, mesmo que você tenha o cuidado de encriptar os dados enviados. Isto pode ser feito não apenas lendo o cabeçalho IP, mas também através da leitura das suas requisições a servidores DNS.

Lorem ipsum dolor sit amet, consectetuer adipiscing elit. Ut purus elit, vestibulum ut, placerat ac, adipiscing vitae, felis. Curabitur dictum gravida mauris. Nam arcu libero, nonummy eget, consectetuer id, vulputate a, magna. Donec vehicula augue eu neque. Pellentesque habitant morbi tristique senectus et netus et malesuada fames ac turpis egestas. Mauris ut leo. Cras viverra metus rhoncus sem. Nulla et lectus vestibulum urna fringilla ultrices. Phasellus eu tellus sit amet tortor gravida placerat. Integer sapien est, iaculis in, pretium quis, viverra ac, nunc. Praesent eget sem vel leo ultrices bibendum. Aenean faucibus. Morbi dolor nulla, malesuada eu, pulvinar at, mollis ac, nulla. Curabitur auctor semper nulla. Donec varius orci eget risus. Duis nibh mi, congue eu, accumsan eleifend, sagittis quis, diam. Duis eget orci sit amet orci dignissim rutrum.

4.2.3 Web Bugs

Ao acessar um site como o Facebook, há na página dispositivos que servem para parceiros do Facebook registrarem sua presença. Ao mesmo tempo em que você requisita a página do Facebook, você automaticamente requisita uma outra página, contida dentro do Facebook, mas hospedada por outro servidor. Esta requisição contém informações que só seriam visíveis ao Facebook, e passam a ser compartilhadas com esses parceiros. Estes parceiros também instalam estes "dispositivos"em outros sites, como sites de e-commerce, por exemplo. Desta forma, o parceiro do Facebook consegue saber o que você está buscando numa loja online, e aí na hora que você utiliza o Facebook, ele apresenta um anúncio parecido com o que você procurou, aumentando as chances de você clicar. Estes dados que traçam seu perfil consumidor não necessariamente são protegidos. Pode-se até vender este tipo de informação.

http://en.wikipedia.org/wiki/Web(underline)bug http://disconnect.me https://www.eff.org/deeplinks/2012/04/4

simple-changes-protect-your-privacy-online http://www.wikihow.com/Prevent-People-from-Tracking-You-on-the-Internet

4.3 Aquisição dos dados já enviados

Pode-se investigar um indivíduo sem necessariamente ele estar conectado na Internet naquele momento. O espião pode siimplesmente conseguir acesso a registros que ficam armazenados em dispositivos da infraestrutura da rede, internos ao ISP, por exemplo. Ou então, acessar dados mais ricos, registros de utilização de um serviço como uma rede social, mensageiro instantâneo ou e-mail.

CAPÍTULO 5

Métodos para contornar censura na Internet

5.1 Proxy

5.1.1 Proxy simples

Vantagens:

Lorem ipsum dolor sit amet, consectetuer adipiscing elit. Ut purus elit, vestibulum ut, placerat ac, adipiscing vitae, felis. Curabitur dictum gravida mauris. Nam arcu libero, nonummy eget, consectetuer id, vulputate a, magna. Donec vehicula augue eu neque. Pellentesque habitant morbi tristique senectus et netus et malesuada fames ac turpis egestas. Mauris ut leo. Cras viverra metus rhoncus sem. Nulla et lectus vestibulum urna fringilla ultrices. Phasellus eu tellus sit amet tortor gravida placerat. Integer sapien est, iaculis in, pretium quis, viverra ac, nunc. Praesent eget sem vel leo ultrices bibendum. Aenean faucibus. Morbi dolor nulla, malesuada eu, pulvinar at, mollis ac, nulla. Curabitur auctor semper nulla. Donec varius orci eget risus. Duis nibh mi, congue eu, accumsan eleifend, sagittis quis, diam. Duis eget orci sit amet orci dignissim rutrum.

Desvantagens:

Lorem ipsum dolor sit amet, consectetuer adipiscing elit. Ut purus elit, vestibulum ut, placerat ac, adipiscing vitae, felis. Curabitur dictum gravida mauris. Nam arcu libero, nonummy eget, consectetuer id, vulputate a, magna. Donec vehicula augue eu neque. Pellentesque habitant morbi tristique senectus et netus et malesuada fames ac turpis egestas. Mauris ut leo. Cras viverra metus rhoncus sem. Nulla et lectus vestibulum urna fringilla ultrices. Phasellus eu tellus sit amet tortor gravida placerat. Integer sapien est, iaculis in, pretium quis, viverra ac, nunc. Praesent eget sem vel leo ultrices bibendum. Aenean faucibus. Morbi dolor nulla, malesuada eu, pulvinar at, mollis ac, nulla. Curabitur auctor semper nulla. Donec varius orci eget risus. Duis nibh mi, congue eu, accumsan eleifend, sagittis quis, diam. Duis eget orci sit amet orci dignissim rutrum.

Popularidade:

Lorem ipsum dolor sit amet, consectetuer adipiscing elit. Ut purus elit, vestibulum ut, placerat ac, adipiscing vitae, felis. Curabitur dictum gravida mauris. Nam arcu libero, nonummy eget, consectetuer id, vulputate a, magna. Donec vehicula augue eu neque. Pellentesque habitant morbi tristique senectus et netus et malesuada fames ac turpis egestas. Mauris ut leo. Cras viverra metus rhoncus sem. Nulla et lectus vestibulum urna fringilla ultrices. Phasellus eu tellus sit amet tortor gravida placerat. Integer sapien est, iaculis in, pretium quis, viverra ac, nunc. Praesent eget sem vel leo ultrices bibendum. Aenean faucibus. Morbi dolor nulla, malesuada eu, pulvinar at, mollis ac, nulla. Curabitur auctor semper nulla. Donec varius orci eget risus.

Duis nibh mi, congue eu, accumsan eleifend, sagittis quis, diam. Duis eget orci sit amet orci dignissim rutrum.

5.1.2 Proxy+SSL

Lorem ipsum dolor sit amet, consectetuer adipiscing elit. Ut purus elit, vestibulum ut, placerat ac, adipiscing vitae, felis. Curabitur dictum gravida mauris. Nam arcu libero, nonummy eget, consectetuer id, vulputate a, magna. Donec vehicula augue eu neque. Pellentesque habitant morbi tristique senectus et netus et malesuada fames ac turpis egestas. Mauris ut leo. Cras viverra metus rhoncus sem. Nulla et lectus vestibulum urna fringilla ultrices. Phasellus eu tellus sit amet tortor gravida placerat. Integer sapien est, iaculis in, pretium quis, viverra ac, nunc. Praesent eget sem vel leo ultrices bibendum. Aenean faucibus. Morbi dolor nulla, malesuada eu, pulvinar at, mollis ac, nulla. Curabitur auctor semper nulla. Donec varius orci eget risus. Duis nibh mi, congue eu, accumsan eleifend, sagittis quis, diam. Duis eget orci sit amet orci dignissim rutrum.

5.1.3 Proxies múltiplos

Lorem ipsum dolor sit amet, consectetuer adipiscing elit. Ut purus elit, vestibulum ut, placerat ac, adipiscing vitae, felis. Curabitur dictum gravida mauris. Nam arcu libero, nonummy eget, consectetuer id, vulputate a, magna. Donec vehicula augue eu neque. Pellentesque habitant morbi tristique senectus et netus et malesuada fames ac turpis egestas. Mauris ut leo. Cras viverra metus rhoncus sem. Nulla et lectus vestibulum urna fringilla ultrices. Phasellus eu tellus sit amet tortor gravida placerat. Integer sapien est, iaculis in, pretium quis, viverra ac, nunc. Praesent eget sem vel leo ultrices bibendum. Aenean faucibus. Morbi dolor nulla, malesuada eu, pulvinar at, mollis ac, nulla. Curabitur auctor semper nulla. Donec varius orci eget risus. Duis nibh mi, congue eu, accumsan eleifend, sagittis quis, diam. Duis eget orci sit amet orci dignissim rutrum.

5.1.4 Tor

Lorem ipsum dolor sit amet, consectetuer adipiscing elit. Ut purus elit, vestibulum ut, placerat ac, adipiscing vitae, felis. Curabitur dictum gravida mauris. Nam arcu libero, nonummy eget, consectetuer id, vulputate a, magna. Donec vehicula augue eu neque. Pellentesque habitant morbi tristique senectus et netus et malesuada fames ac turpis egestas. Mauris ut leo. Cras viverra metus rhoncus sem. Nulla et lectus vestibulum urna fringilla ultrices. Phasellus eu tellus sit amet tortor gravida placerat. Integer sapien est, iaculis in, pretium quis, viverra ac, nunc. Praesent eget sem vel leo ultrices bibendum. Aenean faucibus. Morbi dolor nulla, malesuada eu, pulvinar at, mollis ac, nulla. Curabitur auctor semper nulla. Donec varius orci eget risus. Duis nibh mi, congue eu, accumsan eleifend, sagittis quis, diam. Duis eget orci sit amet orci dignissim rutrum.

5.1.5 Tor+SSL

Lorem ipsum dolor sit amet, consectetuer adipiscing elit. Ut purus elit, vestibulum ut, placerat ac, adipiscing vitae, felis. Curabitur dictum gravida mauris. Nam arcu libero, nonummy eget, consectetuer id, vulputate a, magna. Donec vehicula augue eu neque. Pellentesque habitant morbi tristique senectus et netus et malesuada fames ac turpis egestas. Mauris ut leo. Cras viverra metus rhoncus sem. Nulla et lectus vestibulum urna fringilla ultrices. Phasellus eu tellus sit amet tortor gravida placerat. Integer sapien est, iaculis in, pretium quis, viverra ac, nunc. Praesent eget sem vel leo ultrices bibendum. Aenean faucibus. Morbi dolor nulla, malesuada eu, pulvinar at, mollis ac, nulla. Curabitur auctor semper nulla. Donec varius orci eget risus. Duis nibh mi, congue eu, accumsan eleifend, sagittis quis, diam. Duis eget orci sit amet orci dignissim rutrum.

5.2 Acesso via satélite

Lorem ipsum dolor sit amet, consectetuer adipiscing elit. Ut purus elit, vestibulum ut, placerat ac, adipiscing vitae, felis. Curabitur dictum gravida mauris. Nam arcu libero, nonummy eget, consectetuer id, vulputate a, magna. Donec vehicula augue eu neque. Pellentesque habitant morbi tristique senectus et netus et malesuada fames ac turpis egestas. Mauris ut leo. Cras viverra metus rhoncus sem. Nulla et lectus vestibulum urna fringilla ultrices. Phasellus eu tellus sit amet tortor gravida placerat. Integer sapien est, iaculis in, pretium quis, viverra ac, nunc. Praesent eget sem vel leo ultrices bibendum. Aenean faucibus. Morbi dolor nulla, malesuada eu, pulvinar at, mollis ac, nulla. Curabitur auctor semper nulla. Donec varius orci eget risus. Duis nibh mi, congue eu, accumsan eleifend, sagittis quis, diam. Duis eget orci sit amet orci dignissim rutrum.

5.3 Análise comparativa

5.3.1 Critérios de avaliação

Lorem ipsum dolor sit amet, consectetuer adipiscing elit. Ut purus elit, vestibulum ut, placerat ac, adipiscing vitae, felis. Curabitur dictum gravida mauris. Nam arcu libero, nonummy eget, consectetuer id, vulputate a, magna. Donec vehicula augue eu neque. Pellentesque habitant morbi tristique senectus et netus et malesuada fames ac turpis egestas. Mauris ut leo. Cras viverra metus rhoncus sem. Nulla et lectus vestibulum urna fringilla ultrices. Phasellus eu tellus sit amet tortor gravida placerat. Integer sapien est, iaculis in, pretium quis, viverra ac, nunc. Praesent eget sem vel leo ultrices bibendum. Aenean faucibus. Morbi dolor nulla, malesuada eu, pulvinar at, mollis ac, nulla. Curabitur auctor semper nulla. Donec varius orci eget risus. Duis nibh mi, congue eu, accumsan eleifend, sagittis quis, diam. Duis eget orci sit amet orci dignissim rutrum.

5.3.2 Resultados

Lorem ipsum dolor sit amet, consectetuer adipiscing elit. Ut purus elit, vestibulum ut, placerat ac, adipiscing vitae, felis. Curabitur dictum gravida mauris. Nam arcu libero, nonummy eget, consectetuer id, vulputate a, magna. Donec vehicula augue eu neque. Pellentesque habitant morbi tristique senectus et netus et malesuada fames ac turpis egestas. Mauris ut leo. Cras viverra metus rhoncus sem. Nulla et lectus vestibulum urna fringilla ultrices. Phasellus eu tellus sit amet tortor gravida placerat. Integer sapien est, iaculis in, pretium quis, viverra ac, nunc. Praesent eget sem vel leo ultrices bibendum. Aenean faucibus. Morbi dolor nulla, malesuada eu, pulvinar at, mollis ac, nulla. Curabitur auctor semper nulla. Donec varius orci eget risus. Duis nibh mi, congue eu, accumsan eleifend, sagittis quis, diam. Duis eget orci sit amet orci dignissim rutrum.

CAPÍTULO 6

Métodos para contornar vigilância na Internet

6.1 Proxy

6.1.1 Proxy simples

Lorem ipsum dolor sit amet, consectetuer adipiscing elit. Ut purus elit, vestibulum ut, placerat ac, adipiscing vitae, felis. Curabitur dictum gravida mauris. Nam arcu libero, nonummy eget, consectetuer id, vulputate a, magna. Donec vehicula augue eu neque. Pellentesque habitant morbi tristique senectus et netus et malesuada fames ac turpis egestas. Mauris ut leo. Cras viverra metus rhoncus sem. Nulla et lectus vestibulum urna fringilla ultrices. Phasellus eu tellus sit amet tortor gravida placerat. Integer sapien est, iaculis in, pretium quis, viverra ac, nunc. Praesent eget sem vel leo ultrices bibendum. Aenean faucibus. Morbi dolor nulla, malesuada eu, pulvinar at, mollis ac, nulla. Curabitur auctor semper nulla. Donec varius orci eget risus. Duis nibh mi, congue eu, accumsan eleifend, sagittis quis, diam. Duis eget orci sit amet orci dignissim rutrum.

6.1.2 Proxy+SSL

Lorem ipsum dolor sit amet, consectetuer adipiscing elit. Ut purus elit, vestibulum ut, placerat ac, adipiscing vitae, felis. Curabitur dictum gravida mauris. Nam arcu libero, nonummy eget, consectetuer id, vulputate a, magna. Donec vehicula augue eu neque. Pellentesque habitant morbi tristique senectus et netus et malesuada fames ac turpis egestas. Mauris ut leo. Cras viverra metus rhoncus sem. Nulla et lectus vestibulum urna fringilla ultrices. Phasellus eu tellus sit amet tortor gravida placerat. Integer sapien est, iaculis in, pretium quis, viverra ac, nunc. Praesent eget sem vel leo ultrices bibendum. Aenean faucibus. Morbi dolor nulla, malesuada eu, pulvinar at, mollis ac, nulla. Curabitur auctor semper nulla. Donec varius orci eget risus. Duis nibh mi, congue eu, accumsan eleifend, sagittis quis, diam. Duis eget orci sit amet orci dignissim rutrum.

6.1.3 Proxies múltiplos

Lorem ipsum dolor sit amet, consectetuer adipiscing elit. Ut purus elit, vestibulum ut, placerat ac, adipiscing vitae, felis. Curabitur dictum gravida mauris. Nam arcu libero, nonummy eget, consectetuer id, vulputate a, magna. Donec vehicula augue eu neque. Pellentesque habitant morbi tristique senectus et netus et malesuada fames ac turpis egestas. Mauris ut leo. Cras viverra metus rhoncus sem. Nulla et lectus vestibulum urna fringilla ultrices. Phasellus eu tellus sit amet tortor gravida placerat. Integer sapien est, iaculis in, pretium quis, viverra ac,

nunc. Praesent eget sem vel leo ultrices bibendum. Aenean faucibus. Morbi dolor nulla, malesuada eu, pulvinar at, mollis ac, nulla. Curabitur auctor semper nulla. Donec varius orci eget risus. Duis nibh mi, congue eu, accumsan eleifend, sagittis quis, diam. Duis eget orci sit amet orci dignissim rutrum.

6.1.4 Tor

Lorem ipsum dolor sit amet, consectetuer adipiscing elit. Ut purus elit, vestibulum ut, placerat ac, adipiscing vitae, felis. Curabitur dictum gravida mauris. Nam arcu libero, nonummy eget, consectetuer id, vulputate a, magna. Donec vehicula augue eu neque. Pellentesque habitant morbi tristique senectus et netus et malesuada fames ac turpis egestas. Mauris ut leo. Cras viverra metus rhoncus sem. Nulla et lectus vestibulum urna fringilla ultrices. Phasellus eu tellus sit amet tortor gravida placerat. Integer sapien est, iaculis in, pretium quis, viverra ac, nunc. Praesent eget sem vel leo ultrices bibendum. Aenean faucibus. Morbi dolor nulla, malesuada eu, pulvinar at, mollis ac, nulla. Curabitur auctor semper nulla. Donec varius orci eget risus. Duis nibh mi, congue eu, accumsan eleifend, sagittis quis, diam. Duis eget orci sit amet orci dignissim rutrum.

6.1.5 Tor+SSL

Lorem ipsum dolor sit amet, consectetuer adipiscing elit. Ut purus elit, vestibulum ut, placerat ac, adipiscing vitae, felis. Curabitur dictum gravida mauris. Nam arcu libero, nonummy eget, consectetuer id, vulputate a, magna. Donec vehicula augue eu neque. Pellentesque habitant morbi tristique senectus et netus et malesuada fames ac turpis egestas. Mauris ut leo. Cras viverra metus rhoncus sem. Nulla et lectus vestibulum urna fringilla ultrices. Phasellus eu tellus sit amet tortor gravida placerat. Integer sapien est, iaculis in, pretium quis, viverra ac, nunc. Praesent eget sem vel leo ultrices bibendum. Aenean faucibus. Morbi dolor nulla, malesuada eu, pulvinar at, mollis ac, nulla. Curabitur auctor semper nulla. Donec varius orci eget risus. Duis nibh mi, congue eu, accumsan eleifend, sagittis quis, diam. Duis eget orci sit amet orci dignissim rutrum.

6.1.6 Freenet

https://freenetproject.org/

6.1.7 Freegate

http://www.dit-inc.us/freegate

6.1.8 I2P

Lorem ipsum dolor sit amet, consectetuer adipiscing elit. Ut purus elit, vestibulum ut, placerat ac, adipiscing vitae, felis. Curabitur dictum gravida mauris. Nam arcu libero, nonummy eget, consectetuer id, vulputate a, magna. Donec vehicula augue eu neque. Pellentesque habitant

morbi tristique senectus et netus et malesuada fames ac turpis egestas. Mauris ut leo. Cras viverra metus rhoncus sem. Nulla et lectus vestibulum urna fringilla ultrices. Phasellus eu tellus sit amet tortor gravida placerat. Integer sapien est, iaculis in, pretium quis, viverra ac, nunc. Praesent eget sem vel leo ultrices bibendum. Aenean faucibus. Morbi dolor nulla, malesuada eu, pulvinar at, mollis ac, nulla. Curabitur auctor semper nulla. Donec varius orci eget risus. Duis nibh mi, congue eu, accumsan eleifend, sagittis quis, diam. Duis eget orci sit amet orci dignissim rutrum.

6.2 Esteganografia

Em situações em que o usuário esteja sendo constantemente vigiado e ou perseguido, ainda é possível transmitir informações sigilosas sem levantar tanta suspeita quanto quando se utiliza criptografia pura. Além disso, em alguns países o uso de criptografia é proibido por lei, então mesmo sem conhecer o conteúdo da mensagem, o governo pode prender o cidadão, por apenas utilizar a criptografia.

Esteganografia é o nome dado a técnicas de ocultação de mensagens, onde duas mensagens são enviadas através de um mesmo meio, uma com conteúdo qualquer, banal e outra com conteúdo crítico, a ser escondido. A mensagem que se deseja esconder é apresentada de forma não intuitiva ou invisível sem as devidas ferramentas. Ao leitor desavisado, a mensagem lida será apenas uma e será a desimportante ou banal.

O primeiro uso do termo data de 1499, mas o primeiro registro de utilização deste tipo de técnica data de 400 a.C., tratando-se portanto de técnicas seculares, que foram apenas adaptadas para o mundo dos computadores. Entre as diversas técnicas não-digitais, há a utilização de tinta invisível, que só é revelada sob circunstâncias específicas como alto calor, ou luz especial. Portanto, o remetente pode escrever uma lista de compras, por exemplo, usando tinta normal, e nos espaços em branco que sobrarem, escrever com tinta invisível a mensagem a ser escondida. Obviamente o receptor, e apenas ele, deve conhecer a forma de revelar a mensagem.

No âmbito digital, pode-se por exemplo alterar minimamente o tom de cor de cada pixel de uma imagem. Tais modificações são imperceptíveis para um ser humano, mas são suficientes para guardar um texto inteiro, ou até mesmo uma outra imagem. Para decodificar a mensagem escondida, deve-se utilizar uma ferramenta de extração da mensagem.

6.2.1 Esteganografia utilizada como apoio à vigilância governamental

Algumas impressoras, especialmente as coloridas à *laser*, imprimem pontos amarelos praticamente imperceptíveis em todas as páginas, sem consentimento do usuário. Para o usuário desavisado, estes pontos podem ser entendidos como um defeito na impressora, ou característica estranha do papel. No entanto, estes pontos amarelos são posicionados de forma que guardem uma informação valiosa: a marca e o número de série da impressora utilizada. Desta forma, é possível utilizar a informação para rastrear o dono da impressora e possivelmente quem imprimiu um certo documento. Esta tecnologia foi implementada por grandes companhias como a Xerox, Canon e várias outras, motivados pela preocupação de alguns governos, de que estas impressoras fossem utilizadas para falsificar dinheiro.

6.3 Análise comparativa

http://www.i2p2.de/how(underline)networkcomparisons http://alternativeto.net/software/tor/

6.3.1 Critérios de avaliação

Lorem ipsum dolor sit amet, consectetuer adipiscing elit. Ut purus elit, vestibulum ut, placerat ac, adipiscing vitae, felis. Curabitur dictum gravida mauris. Nam arcu libero, nonummy eget, consectetuer id, vulputate a, magna. Donec vehicula augue eu neque. Pellentesque habitant morbi tristique senectus et netus et malesuada fames ac turpis egestas. Mauris ut leo. Cras viverra metus rhoncus sem. Nulla et lectus vestibulum urna fringilla ultrices. Phasellus eu tellus sit amet tortor gravida placerat. Integer sapien est, iaculis in, pretium quis, viverra ac, nunc. Praesent eget sem vel leo ultrices bibendum. Aenean faucibus. Morbi dolor nulla, malesuada eu, pulvinar at, mollis ac, nulla. Curabitur auctor semper nulla. Donec varius orci eget risus. Duis nibh mi, congue eu, accumsan eleifend, sagittis quis, diam. Duis eget orci sit amet orci dignissim rutrum.

6.3.2 Resultados

Lorem ipsum dolor sit amet, consectetuer adipiscing elit. Ut purus elit, vestibulum ut, placerat ac, adipiscing vitae, felis. Curabitur dictum gravida mauris. Nam arcu libero, nonummy eget, consectetuer id, vulputate a, magna. Donec vehicula augue eu neque. Pellentesque habitant morbi tristique senectus et netus et malesuada fames ac turpis egestas. Mauris ut leo. Cras viverra metus rhoncus sem. Nulla et lectus vestibulum urna fringilla ultrices. Phasellus eu tellus sit amet tortor gravida placerat. Integer sapien est, iaculis in, pretium quis, viverra ac, nunc. Praesent eget sem vel leo ultrices bibendum. Aenean faucibus. Morbi dolor nulla, malesuada eu, pulvinar at, mollis ac, nulla. Curabitur auctor semper nulla. Donec varius orci eget risus. Duis nibh mi, congue eu, accumsan eleifend, sagittis quis, diam. Duis eget orci sit amet orci dignissim rutrum.

Referências Bibliográficas

[Ada06] Carlisle Adams. A classification for privacy techniques. *University of Ottawa Law & Technology Journal*, 3:35–52, 2006.

[Dei13] R.J. Deibert. *Black Code: Inside the Battle for Cyberspace*. McClelland & Stewart, 2013.

[DI10] R.J. Deibert and OpenNet Initiative. *Access Controlled: The Shaping of Power, Rights, and Rule in Cyberspace*. Information Revolution and Global Politics. Mit Press, 2010.

[DMS04] Roger Dingledine, Nick Mathewson, and Paul Syverson. Tor: The second-generation onion router. In *Proceedings of the 13th USENIX Security Symposium*, August 2004.

[ED93] PHILIP ELMER-DEWITT. First nation in cyberspace. TIME Magazine, December 1993.

[FRA13] BERNARDO MELLO FRANCO. Pressionado, obama promete abrir informacoes sobre vigilancia na internet. Folha de Sao Paulo, June 2013.

[Mor12] E. Morozov. *The Net Delusion: The Dark Side of Internet Freedom*. PublicAffairs, 2012.

Este volume foi tipografado em LaTeX na classe UFPEThesis (www.cin.ufpe.br/~paguso/ufpethesis).