



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 direitos humanos, praticado pelos seus governantes.

Teste cite [3] e ref [8].

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

Abstract

Lorem ipsum dolor sit amet, consectetur adipiscing elit. Ut purus elit, vestibulum ut, placerat ac, adipiscing vitae, felis. Curabitur dictum gravida mauris. Nam arcu libero, nonummy eget, consectetur 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

1	Introdução	1
1.1	Motivação e Contextualização	1
1.1.1	A influência da Internet na sociedade	1
1.1.2	O perigo da ignorância sobre o funcionamento da Internet	3
1.2	Objetivos	3
1.3	Estrutura do trabalho	3
2	Fundamentos do funcionamento e infraestrutura da Internet	5
2.1	Analogia com serviço postal	5
2.2	O uso da criptografia na Internet	6
2.3	Pacotes IP	7
2.3.1	Como funcionam a Web e os servidores de nomes	7
2.4	Conceitos básicos	8
3	Censura na Internet	11
3.1	Remoção de conteúdo	11
3.1.1	Terceirização da censura	12
3.1.2	Legitimidade da censura	12
3.2	Bloqueio de acesso a conteúdo	12
3.2.1	DNS Poisoning	12
3.2.2	Filtragem de pacotes: Bloqueio a IPs	14
3.2.3	Filtragem de pacotes: Inspeção de pacotes	14
3.3	Empresas que lucram com a censura e a vigilância	14
3.4	A relação entre vigilância e censura – Autocensura	16
4	Vigilância na Internet	17
4.1	Transmissão involuntária dos dados	17
4.1.1	Infecção do computador	17
4.1.2	Infection Proxies	18
4.2	Interceptação dos dados em trânsito	18
4.2.1	Interceptação total dos dados	18
4.2.2	Descoberta dos seus destinatários	18
4.2.3	Web Bugs	18
4.3	Aquisição dos dados já enviados	19

5	Métodos para contornar vigilância e censura na Internet	21
5.1	Proxy	21
5.1.1	Proxies múltiplos	21
5.1.1.1	Proxies encadeados	21
5.1.1.2	Proxies em paralelo	21
5.1.2	Tor	21
5.1.3	Tor+SSL	22
5.1.4	Freenet	23
5.1.5	Freemove	23
5.1.6	I2P	23
5.2	Acesso via satélite	23
5.3	Esteganografia	23
5.3.1	Esteganografia utilizada como apoio à vigilância governamental	24
5.4	Análise comparativa	24
5.4.1	Critérios de avaliação	24
5.4.2	Resultados	25

Lista de Figuras

1.1	Página com transmissão do Mídia NINJA ao vivo	2
1.2	Gráfico do Arab Social Media Report	4
3.1	Página recebida ao tentar acessar sites proibidos nos Emirados Árabes Unidos	13
3.2	Imagem capturada da página da Blue Coat	15
5.1	Imagem resposta com o texto I'm behind seven proxies	22

CAPÍTULO 1

Introdução

1.1 Motivação e Contextualização

1.1.1 A influência da Internet na sociedade

Pablo Capilé¹ 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 fazer registros com seu *smartphone*, publicando em um blog ou rede social e mostrando sua visão dos fatos. A maior pluralidade de pontos de vista nas notícias permite que o cidadão faça sua interpretação dos fatos com mais precisão. Dependendo da origem da notícia, haverá atenuação de alguns fatos e destaque em outros, para induzir alguma conclusão específica no leitor. Com diferentes graus de atenuação e destaque, é possível tirar uma “mídia” entre as notícias e se aproximar mais da realidade.

A Figura 1.1 mostra um exemplo de *streaming* de vídeo, feito pela Mídia NINJA de Pernambuco. Nela podemos perceber uma aproximação maior do repórter com o público, através do campo de comentários, que inclusive é utilizado pelo repórter como fonte de informações. O que o público informa ao repórter da Mídia NINJA, pode acabar influenciando na transmissão, às vezes comandando o que deve ser mostrado, ou avisando de algum risco que o repórter pode correr.

Em regimes autoritários, a influência sobre as fontes de notícia são muito importantes para o governo garantir a quietude da população e a manutenção do poder. Sem notícias sobre manifestos e revoluções, a população não se inspira e não se “contamina” com ideias subversivas. A Internet é um meio mais difícil de controlar do que as transmissoras de rádio e TV. Nela, os cidadãos podem ouvir e expressar opiniões de descontentamento, tornando o povo mais unido a ponto de derrubar governos há décadas estabelecidos.

Um exemplo do impacto da Internet e das redes sociais na sociedade são as revoluções recentes ocorridas no norte da África e Oriente Médio, coletivamente conhecidas como A Primavera Árabe. As novas mídias são vistas e usadas como agentes de mudança na região árabe, segundo pesquisa publicada em [10]. Esse estudo também fez pesquisas de opinião do povo

¹Pablo Capilé é um dos idealizadores do grupo 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 por manifestantes reivindicando passe livre de ônibus. 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 fonte de informação mais atualizada sobre a ocupação da câmara.

árabe sobre as mudanças trazidas pelas redes sociais como se pode ver na Figura 1.2.

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 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. Diferentemente do que se acredita, e este trabalho tentará mostrar o contrário, a Internet não é um espaço público, inviolável e incensurável. Para que a rede esteja a serviço dos cidadãos, é importante que esses cobrem por isso.

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 para monitorar o que todos acessam e publicam. Também serão apresentados alguns métodos para contornar bloqueios e monitoramentos. 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

No Capítulo 2 serão apresentados alguns fundamentos sobre a Internet e seu funcionamento, para tornar o leitor suficientemente familiarizado com a terminologia e conceitos que serão abordados no restante do trabalho. Começando pelo Capítulo 3, serão mostradas diferentes formas que a infraestrutura da Internet pode ser manipulada para evitar que os cidadãos tenham acesso a informações que seu governo considere indesejáveis. Em seguida, no capítulo 4, as técnicas de monitoramento e vigilância do comportamento dos cidadãos na rede serão classificadas e explicadas, ilustrando com exemplos reais. Finalmente, no capítulo 5, serão listadas as principais técnicas utilizadas para burlar a censura configurada pelos governos, assim como dificultar o monitoramento empregado por esses.

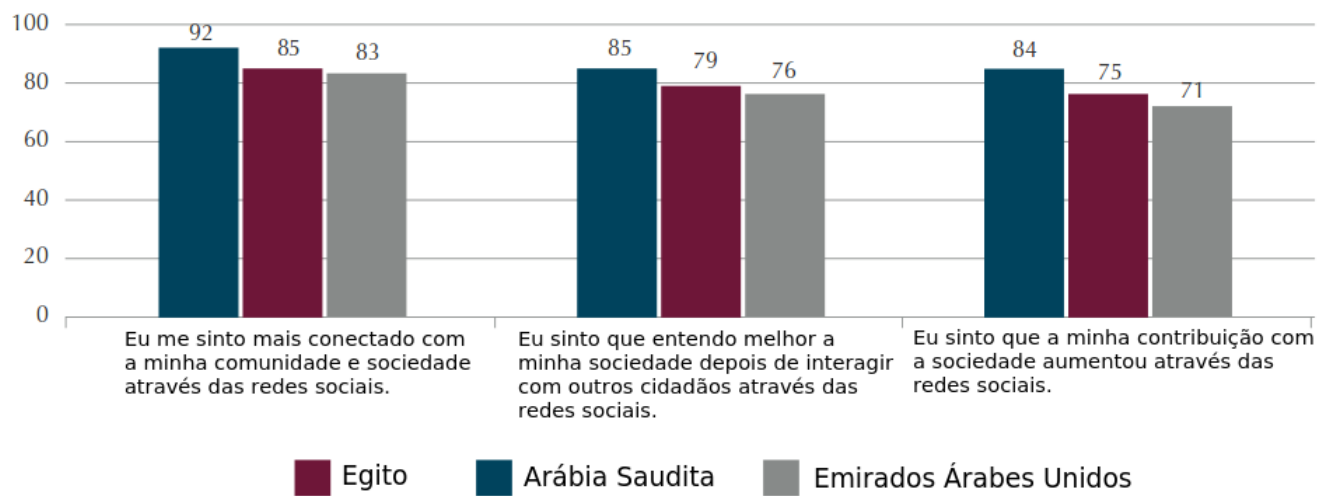


Figura 1.2 Em pesquisa feita pela Dubai School of Government [10], o povo árabe foi consultado a respeito do impacto das redes sociais em sua relação com a sociedade. As porcentagens acima correspondem à quantidade de indivíduos que concordaram com a afirmação escrita abaixo das barras.

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 agentes do governo ou espões contratados para obter informações sigilosas de indivíduos, empresas ou países. 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.

O processo de criptografia de mensagens trata-se apenas de uma série de operações matemáticas executadas sobre a mensagem com o objetivo de descaracterizá-la e tornar o processo inverso uma tarefa virtualmente impossível¹. No entanto, é possível inverter o processo se for utilizada uma chave. Com a chave correta, a mensagem original pode ser obtida facilmente.

Existem dois tipos de chaves para criptografia. Chaves assimétricas e chaves simétricas. No caso das chaves assimétricas, a chave utilizada para esconder a mensagem (criptografar) é diferente daquela utilizada para decodificá-la (descriptografar). No caso das chaves simétricas, a chave para criptografia e descriptografia são idênticas.

Uma aplicação das chaves assimétricas é o conceito de chave pública e chave privada. Um servidor que deseja proteger as mensagens que recebe deve gerar as duas chaves. A chave pública é a chave utilizada para criptografar as mensagens, já a chave privada é aquela utilizada para a descriptografia. Como o próprio nome diz, a chave pública não precisa ser escondida, ela deve estar disponível para quem quiser se comunicar com aquele servidor. O usuário criptografa a mensagem usando a chave pública e envia para o servidor. Já a chave privada deve ser conhecida apenas pelo servidor que a gerou e deve ser protegida a qualquer custo. Somente ela é capaz de descriptografar as mensagens criptografadas com a chave pública. Muitas vezes se utilizam chaves assimétricas apenas para iniciar uma comunicação e combinar uma chave simétrica que apenas os dois conheçam.

Um risco da utilização de chaves públicas e privadas é o conhecido ataque *man in the middle* (homem no meio, em inglês). Como o nome diz, trata-se de uma forma de ouvir a conversa, posicionando-se entre as duas entidades que desejam se comunicar. Para o servidor o atacante finge ser o usuário, e para o usuário ele finge ser o servidor, funcionando como uma

¹Um exemplo de operação que é fácil de ser calculada seria o produto entre dois números primos muito grandes. Realizar este cálculo é simples e qualquer computador é capaz. No entanto, conhecendo apenas o resultado, encontrar quais foram os números utilizados na multiplicação é uma tarefa difícil até mesmo para supercomputadores. É possível, mas pode levar anos, talvez séculos, sendo na prática, impossível de reverter o processo para fins práticos.

ponte entre eles sem que percebam. Primeiro, o elemento mal intencionado induz o usuário utilizar uma chave pública diferente daquela realmente oferecida pelo servidor. Esta chave pública é na verdade uma gerada pelo agente do ataque, cuja chave privada correspondente ele conhece. O que ele faz então é se passar pelo servidor, recebendo os pacotes que o usuário envia, descriptografando-os, lendo-os e criptografando-os novamente, utilizando a chave pública verdadeira do servidor, e os envia, fingindo ser o usuário.

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

Quando acessamos um website como `www.loremipsum.com/posts/3`, primeiro é enviado um pacote ao computador (também chamado de servidor) que contém a página procurada.

O conteúdo deste pacote é um pedido, requisitando um certo recurso. Neste caso . 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 nomes associados a endereços IP. Assim, em vez de decorarmos que o endereço do Google é 74.125.234.240, basta que decoremos seu nome: *www.google.com*.

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.

Quando digitamos apenas um nome como *www.youtube.com* na página de endereços, por padrão nos é apresentada a sua página inicial. No entanto, podemos querer acessar uma página (ou recurso) específica. Se acessarmos *www.youtube.com/watch?v=b-gG5qmXFUA* estamos pedindo ao Youtube o recurso *"/watch?v=b-gG5qmXFUA"*. Então nosso navegador fica encarregado de consultar um servidor DNS, transformar o nome *www.youtube.com* em um endereço IP, e mandar um pacote para este IP pedindo o recurso *"/watch?v=b-gG5qmXFUA"*. Por ser possível acessar recursos de servidores, estes endereços WWW muitas vezes são chamados de URL (*Universal Resource Location*).

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).

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, sendo possivelmente penalizado 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. 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, a remoção é legal.

No entanto, a lei dos países diferem e muitas vezes o conteúdo pode estar hospedado em outro país com legislação diferente. Neste caso, tudo que o governo 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 endereços 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.

A Figura 3.1 mostra um exemplo do que acontece nos Emirados Árabes Unidos quando se acessa um site proibido pelo governo.



خطر!

تصفح بأمان!

عذرا، هذا الموقع غير متاح في دولة الإمارات العربية المتحدة.

تشكل شبكة الانترنت وسيلة للتواصل والمعرفة وخدمة متطلبات حياتنا اليومية. وقد تم حجب الموقع الذي ترغب بدخوله لاشتراكه محتوى مدرج تحت "فئات المحتويات المحظورة" حسب تصنيف "السياسة التنظيمية لإدارة النفاذ للإنترنت" لهيئة تنظيم الاتصالات بدولة الإمارات العربية المتحدة.

إذا كانت لديك وجهة نظر مختلفة، الرجاء [انقر هنا](#).

Surf Safely!

This website is not accessible in the UAE.

The Internet is a powerful medium for communication, sharing and serving our daily learning needs. However, the site you are trying to access contains content that is prohibited under the 'Internet Access Management Regulatory Policy' of the Telecommunications Regulatory Authority of the United Arab Emirates

If you believe the website you are trying to access does not contain any such content, please [click here](#).

© 2009 Lamtlara FZ LLC.

Figura 3.1 Com textos em árabe e em inglês, avisa-se que a Internet é um poderoso meio de comunicação, compartilhamento e de aprendizado diário. No entanto, o conteúdo que o usuário está tentando acessar contém conteúdo proibido pela “Política Reguladora de Gerenciamento de Acesso à Internet”, da Autoridade Reguladora de Telecomunicações dos Emirados Árabes Unidos.

3.2.2 Filtragem de pacotes: 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 alguns servidores. Esta é uma forma mais eficaz de censura, visto que torna-se impossível estabelecer conexão com algumas páginas, se a requisição partir de dentro do país a ser censurado. Um exemplo de uso desta técnica foi percebido por pesquisadores em [1], em que nas vésperas das eleições presidenciais em Junho de 2013, não se podia acessar um site local de notícias <http://presstv.ir>, nem o *The Guardian*, nem o *Le Monde*. Há no entanto, formas de se utilizar um intermediário para burlar o bloqueio governamental. Mais informações sobre estas técnicas estão presentes no Capítulo 5.

3.2.3 Filtragem de pacotes: Inspeção de pacotes

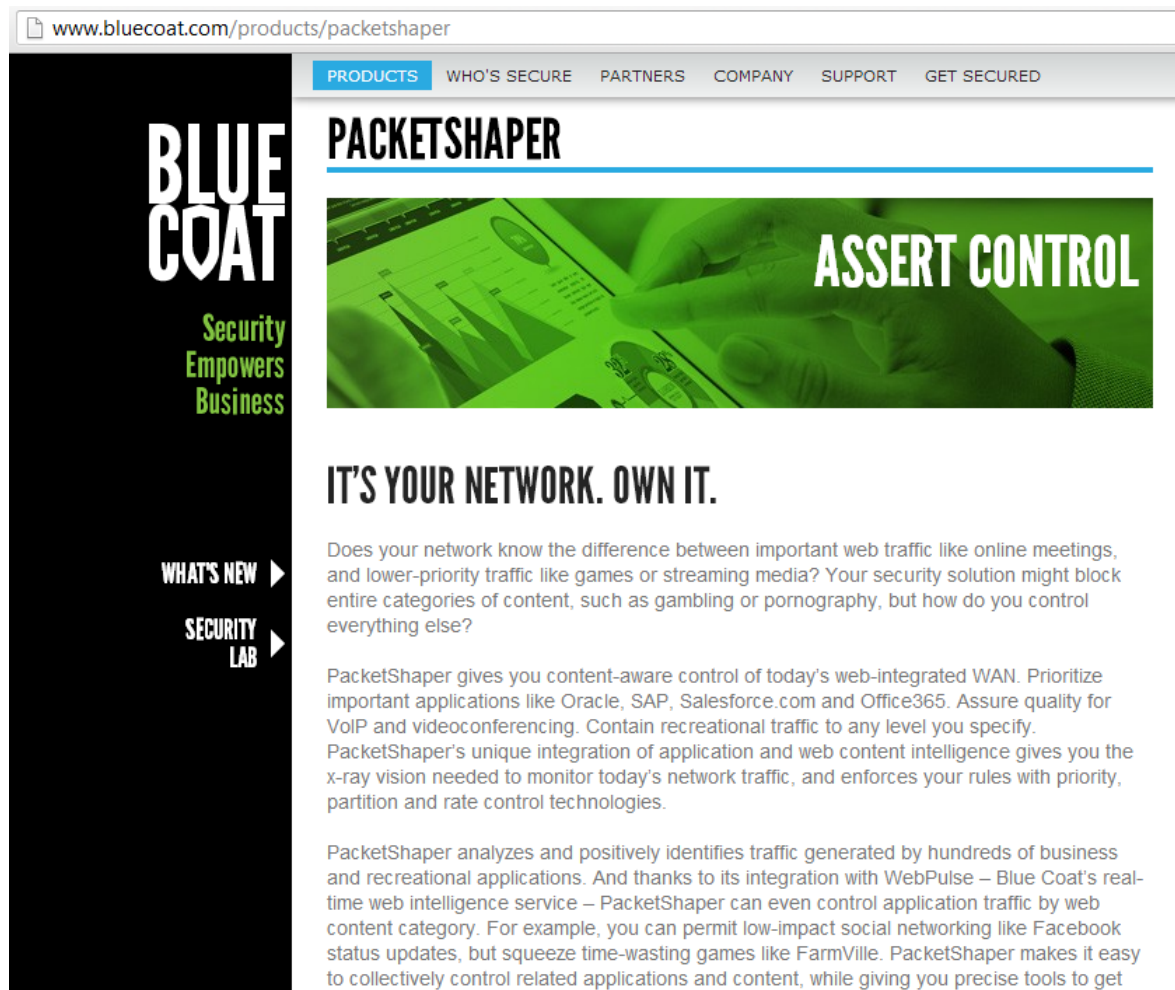
Também é possível filtrar pacotes não apenas pelos endereços envolvidos, mas também pelo conteúdo da mensagem. Esta técnica é conhecida como *Deep Packet Inspection* e é utilizada por alguns provedores de Internet, inclusive no Brasil, para limitar o uso de serviços como *Torrent* e *streaming* de vídeos. O Governo Chinês vai além e não só detecta que tipo de serviço os cidadãos utilizam, mas também que conteúdo eles acessam e transmitem na rede. De acordo com os experimentos feitos em [7], na China não é possível buscar no Google por certas palavras. Ao clicar no botão de busca, é exibida uma mensagem de erro, como se a conexão tivesse sido resetada. Além disso, o usuário não consegue voltar a acessar o Google por cerca de quinze minutos. A Wikipédia inclusive mantém uma lista de quais palavras são censuradas na China em [2].

3.3 Empresas que lucram com a censura e a vigilância

Andy Müller-Maguhn, co-autor do livro *Cypherpunks* ([4]) de Julian Assange, é fundador do site *Bugged Planet* - <http://buggedplanet.info> (Planeta grampeado, em inglês). Lá há uma página no formato *wiki*, colaborativa, onde se compartilham informações sobre vigilância na Internet, incluindo listas de empresas e pessoas que ganham dinheiro com este nicho mercadológico.

Uma delas é a *Blue Coat*, alvo de pesquisas como [11], [9] e [5]. É um exemplo de empresa que produz tecnologia classificada como de “uso dual”. Ou seja, pode ter usos pacíficos e benéficos, assim como usos militares e violentos. Um exemplo de tecnologia de uso dual são os foguetes, que podem ser utilizados para levar homens ao espaço, ou para lançar satélites, como também serem utilizados como armas, como mísseis de longo alcance.

Os dispositivos da *Blue Coat*, podem ser utilizados para gerenciar a rede interna de uma empresa, evitando que funcionários acessem conteúdo inadequado para a realização de suas atividades, ou para garantir o desempenho e segurança da rede. Da mesma forma, pode ser instalado nas fronteiras da Internet de um país e monitorar o tráfego de todos os cidadãos, assim como filtrar o que eles podem acessar. Na Figura 3.2 é mostrada a página da empresa, apresentando seus produtos.



www.bluecoat.com/products/packetshaper

PRODUCTS WHO'S SECURE PARTNERS COMPANY SUPPORT GET SECURED

BLUE COAT

Security Empowers Business

PACKETSHAPER

ASSERT CONTROL

IT'S YOUR NETWORK. OWN IT.

Does your network know the difference between important web traffic like online meetings, and lower-priority traffic like games or streaming media? Your security solution might block entire categories of content, such as gambling or pornography, but how do you control everything else?

PacketShaper gives you content-aware control of today's web-integrated WAN. Prioritize important applications like Oracle, SAP, Salesforce.com and Office365. Assure quality for VoIP and videoconferencing. Contain recreational traffic to any level you specify. PacketShaper's unique integration of application and web content intelligence gives you the x-ray vision needed to monitor today's network traffic, and enforces your rules with priority, partition and rate control technologies.

PacketShaper analyzes and positively identifies traffic generated by hundreds of business and recreational applications. And thanks to its integration with WebPulse – Blue Coat's real-time web intelligence service – PacketShaper can even control application traffic by web content category. For example, you can permit low-impact social networking like Facebook status updates, but squeeze time-wasting games like FarmVille. PacketShaper makes it easy to collectively control related applications and content, while giving you precise tools to get

Figura 3.2 Texto legenda imagem Blue Coat

Foi descoberto que dispositivos da *Blue Coat* eram utilizados pelo governo Sírio, conhecido por perseguir civis contrários ao governo de Bashar Al-Assad. Os mesmos dispositivos foram descobertos sendo utilizados por vários outros países do oriente médio, Ásia e África, segundo relatório do *Citizen Lab* da Universidade de Toronto ([9]).

3.4 A relação entre vigilância e censura – Autocensura

Ronald Deibert em [6] compara o sistema de censura chinês ao livro 1984 de George Orwell e ao conceito de penitenciária idealizado por Jeremy Bentham, o Pan-óptico. No livro de George Orwell, o “Big Brother” se mostra presente em vários momentos do dia-a-dia dos cidadãos. Logo que acordam, por exemplo, ouvem alguma mensagem do “Big Brother”. Portanto, sentem-se vigiados pois está explícita a presença do vigia. Já no Pan-óptico, todas as celas são construídas lado a lado, formando uma circunferência, de modo a serem igualmente e completamente visíveis a uma torre de vigilância central. Nesta torre os guardas ficam escondidos atrás de venezianas, não sendo possível para os presos saber se estão sendo olhados naquele momento ou não. Ou seja, a intenção é dar a impressão que todos estão sendo vigiados, mesmo havendo poucos guardas. Ronald Deibert diz que o sistema de censura chinês se assemelha mais ao Pan-óptico do que ao “Big Brother” de George Orwell. A vigilância é implícita, o que gera uma auto-censura nas pessoas, por medo de serem pegas, sem saber se estão sendo vigiadas naquele momento ou não.

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 legal¹. 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/>

¹Foi publicado nos principais jornais a história de David Miranda, companheiro do jornalista Glenn Greenwald, que foi detido por autoridades britânicas durante quase nove horas, em um aeroporto de Londres em 18 de agosto de 2013. A lei permite esse tipo de detenção em caso de suspeita de terrorismo, no entanto, estava claro que não havia essa suspeita contra David Miranda. Glenn Greenwald escreveu no The Guardian uma série de notícias revelando os projetos de vigilância eletrônica empregados pelo NSA – Agência Nacional de Segurança dos Estados Unidos. Estes projetos foram publicados por um agente interno, Edward Snowden, que hoje procura asilo político, pois

4.1.2 Infection Proxies

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

4.2 Intercepção dos dados em trânsito

4.2.1 Intercepção 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 intercepção pode ser feita em vários lugares: intercepção 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, consectetur adipiscing elit. Ut purus elit, vestibulum ut, placerat ac, adipiscing vitae, felis. Curabitur dictum gravida mauris. Nam arcu libero, nonummy eget, consectetur 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_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 simplesmente 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.

Métodos para contornar vigilância e censura na Internet

5.1 Proxy

Um proxy funciona como um entregador terceirizado.

Existe ainda a possibilidade de usar proxies múltiplos. Em fóruns de discussão na Internet, quando alguns usuários que conhecem estas técnicas são ameaçados de serem processados por algum motivo, às vezes respondem com uma frase clássica “I’m behind seven proxies”, ou na forma de uma imagem resposta, como na figura 5.1.

5.1.1 Proxies múltiplos

5.1.1.1 Proxies encadeados

5.1.1.2 Proxies em paralelo

5.1.2 Tor

O Tor é classificado por alguns como uma ferramenta de proxy. Na verdade ele utiliza o conceito de proxies, mas aumenta um pouco a complexidade para agregar valores que o Proxy por si só não traz.

O Tor serve para despistar alguém que queira descobrir com quem você se comunica e o que você transmite e recebe pela Internet. Seguindo a analogia da seção 2.1 na página 5, é como se você continuasse usando o serviço postal, mas criptografasse suas mensagens e contratasse secretamente pessoas para servirem como intermediários. Ou seja, se você deseja enviar uma encomenda a alguém em Manaus, você deve enviar primeiro para seu parceiro intermediário em São Paulo, que já sabe que deve reenviar para um outro intermediário em Florianópolis, que por sua vez envia para outro intermediário em Fortaleza, que finalmente envia para o seu destinatário em Recife. Um detalhe importante é que todos esses intermediários trabalham para várias outras pessoas. Ou seja, assim que sua encomenda chega no primeiro intermediário, alguém que estiver vigiando sua comunicação com este intermediário, não saberá quais dos pacotes que ele reenviou é o seu, pois são muitos pacotes que saem dele.

..entrar em mais detalhes técnicos..

O Tor tem alguns defeitos. Caso você e seu destinatário estejam sendo monitorados, é possível determinar se vocês estão se comunicando, através de uma análise estatística.

Outro problema é que o IP dos *relays* é uma informação pública e facilmente pode-se

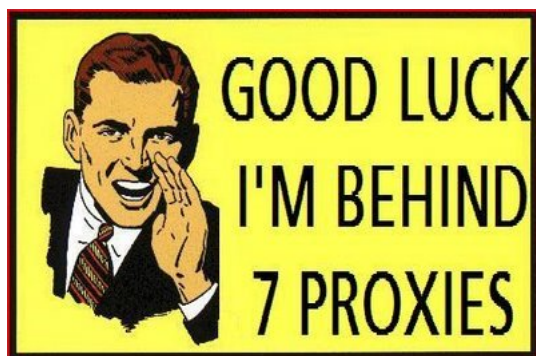


Figura 5.1 Esta expressão surgiu quando alguns hackers mal intencionados invadiram o computador de uma mulher e postaram vídeos e fotos suas em um fórum de discussão chamado *4chan*. Quando descobriu, a mulher foi a este fórum ameaçar que iria denunciar os hackers às autoridades. Foi aí que um deles respondeu com “Boa sorte! Estou por trás de sete proxies!”, significando que seria praticamente impossível localizá-lo. Mais informações sobre esta frase que acabou se tornando um *meme* encontra-se em: <http://knowyourmeme.com/memes/good-luck-im-behind-7-proxies>

bloqueá-los. A criação dos chamados *bridges* foi uma tentativa de solucionar isso. Também é desvantajoso o fato de ser necessário fazer um download para poder aproveitar esta técnica. Se o governo bloquear os sites que oferecem o Tor para download, o cidadão terá dificuldades para conseguí-lo e utilizá-lo.

..citar bloqueio aos relays na china e a criação de bridges..

..citar notícias recentes sobre tor..

FBI admits what we all suspected: it compromised freedom hosting's Tor Servers. <http://arstechnica.com/tech-policy/2013/09/fbi-admits-what-we-all-suspected-it-c>

5.1.3 Tor+SSL

Lorem ipsum dolor sit amet, consectetur adipiscing elit. Ut purus elit, vestibulum ut, placerat ac, adipiscing vitae, felis. Curabitur dictum gravida mauris. Nam arcu libero, nonummy eget, consectetur 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 Freenet

<https://freenetproject.org/>

5.1.5 Freerate

<http://www.dit-inc.us/freerate>

5.1.6 I2P

Lorem ipsum dolor sit amet, consectetur adipiscing elit. Ut purus elit, vestibulum ut, placerat ac, adipiscing vitae, felis. Curabitur dictum gravida mauris. Nam arcu libero, nonummy eget, consectetur 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

..Citar projetos de hackers para criar satélites para acabar com censura na Internet em alguns países <http://www.bbc.co.uk/news/technology-16367042...>

5.3 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 sobram, 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.

5.3.1 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.

5.4 Análise comparativa

[http://www.i2p2.de/how\(networkcomparisons](http://www.i2p2.de/how(networkcomparisons) <http://alternativeto.net/software/tor/>

5.4.1 Critérios de avaliação

Lorem ipsum dolor sit amet, consectetur adipiscing elit. Ut purus elit, vestibulum ut, placerat ac, adipiscing vitae, felis. Curabitur dictum gravida mauris. Nam arcu libero, nonummy eget, consectetur 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.

5.4.2 Resultados

Lorem ipsum dolor sit amet, consectetur adipiscing elit. Ut purus elit, vestibulum ut, placerat ac, adipiscing vitae, felis. Curabitur dictum gravida mauris. Nam arcu libero, nonummy eget, consectetur 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

- [1] La cybercensure iranienne vue de l'intérieur à la veille des élections présidentielles... Powered by Cisco Systems. http://reflets.info/la-cybercensure-iranienne-vue-de-linterieure-a-la-veille_-des-elections-presidentielles-powered-by-cisco-systems/, June 2013. [Online; acessado em 23 de Setembro de 2013].
- [2] List of blacklisted keywords in the People's Republic of China. http://en.wikipedia.org/wiki/List_of_blacklisted_keywords_in_the_People%27s_Republic_of_China, 2013. [Online; acessado em 23 de Setembro de 2013].
- [3] Carlisle Adams. A classification for privacy techniques. *University of Ottawa Law & Technology Journal*, 3:35–52, 2006.
- [4] J. Assange, J. Appelbaum, A. Müller-Maguhn, and J. Zimmermann. *Cypherpunks: Freedom and the Future of the Internet*. OR Books, LLC, 2012.
- [5] bluetouff. #OpSyria: Web censorship technologies in Syria revealed [EN]. <http://reflets.info/opsyria-web-censorship-technologies-in-syria-revealed-en/>, October 2011. [Online; acessado em 23 de Setembro de 2013].
- [6] R.J. Deibert. *Black Code: Inside the Battle for Cyberspace*. McClelland & Stewart, 2013.
- [7] Feng Ding, Zhiqing Yang, Xuelong Chen, and Jianfeng Guo. Effective methods to avoid the internet censorship. In *Parallel Architectures, Algorithms and Programming (PAAP), 2011 Fourth International Symposium on*, pages 67–71, 2011.
- [8] Roger Dingledine, Nick Mathewson, and Paul Syverson. Tor: The second-generation onion router. In *Proceedings of the 13th USENIX Security Symposium*, August 2004.
- [9] Morgan Marquis-Boire, Jakub Dalek, Sarah McKune, Matthew Carrieri, Masashi Crete-Nishihata, Ron Deibert, Saad Omar Khan, Helmi Noman, John Scott-Railton, and Greg Wiseman. Planet Blue Coat: Mapping Global Censorship and Surveillance Tools. <https://citizenlab.org/2013/01/planet-blue-coat-mapping-global-censorship-and-surveillance-tools/>, January 2013. [Online; acessado em 23 de Setembro de 2013].

- [10] Dubai School of Government. Social media in the arab world: Influencing societal and cultural change? <http://www.arabsocialmediareport.com/UserManagement/PDF/ASMR%204%20updated%2029%2008%2012.pdf>, 2012. [Online; acessado em 23 de Setembro de 2013].
- [11] University of Toronto The Citizen Lab. Behind Blue Coat: Investigations of commercial filtering in Syria and Burma. <http://citizenlab.org/2011/11/behind-blue-coat/>, November 2011. [Online; acessado em 23 de Setembro de 2013].

