Projeto Tor

2013-1 – UFRJ – Redes I

Alunos: Jhonatas Alfradique, Hugo Klin, Guilherme Almeida

O que é Tor?

- Tor (The Onion Router, traduzido por “O roteador Cebola”) é uma rede de túneis que permite as pessoas ter segurança e privacidade na internet.
- O principal objetivo do projeto é manter a privacidade e a segurança de seus usuários. Indivíduos usam Tor para se comunicar com seus familiares ou acessarem algum site ou serviço que estejam bloqueados pelo seu provedor de internet.

O que é Tor?

- O Tor-cliente é um programa que deve ser instalado na máquina do usuário, que funciona como um sock proxy.
- A partir daí, o Tor irá rotear todo o tráfego do computador através de túneis http, até a rede convencional.
- Ou seja, Tor é um projeto que visa a segurança e o anonimato. E a forma de utilizá-la é através de um programa que se conecta a rede Tor. Lembrando que cada máquina conectada a rede, se torna um roteador nesta rede.

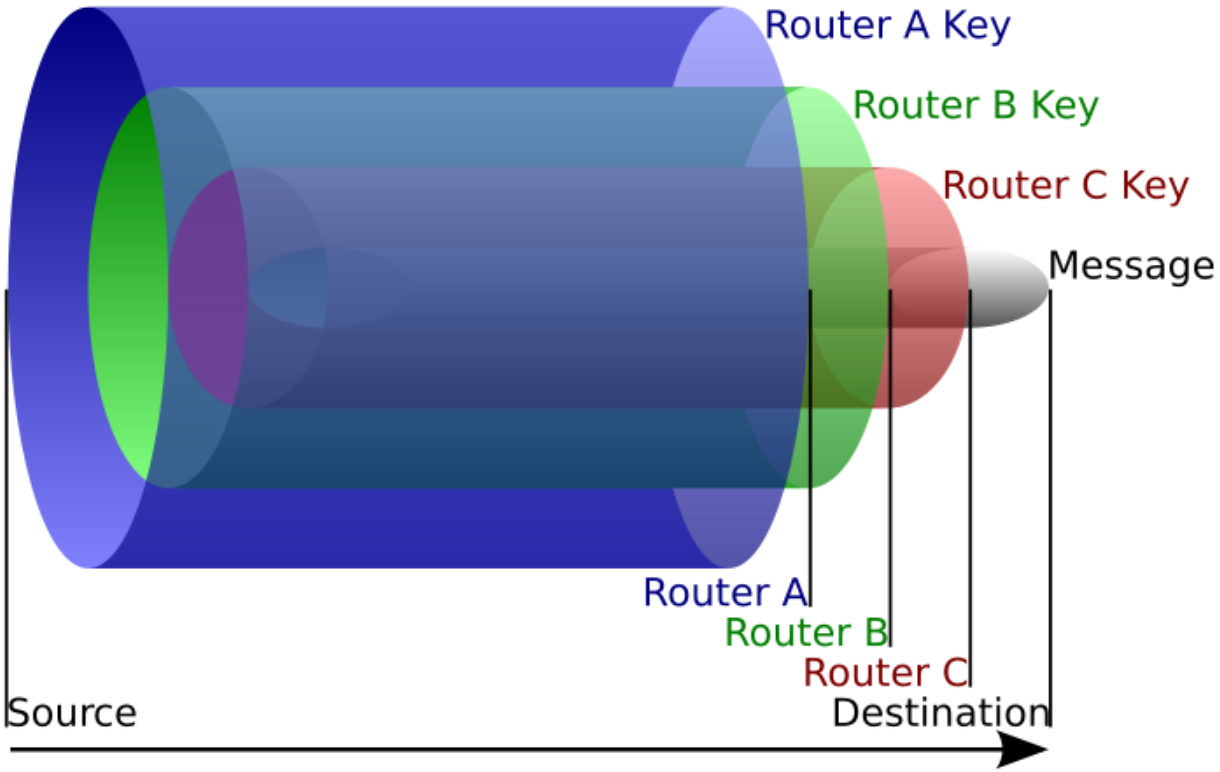
Funcionamento

- O Tor é, essencialmente, um serviço de comunicação anonima através de circuitos virtuais, baseado na técnica de Onion Routing.
- Onion Routing é uma rede sobreposta distribuída, projetada para aplicativos baseados em TCP
- Os clientes escolhem um caminho através da rede e constroem um circuito virtual, em que cada nó ("onion router", ou "OR") no caminho conhece o seu antecessor e sucessor, mas nenhum outro nó no circuito

Onion Routing

- Os fluxos de tráfego no circuito são constituídos de células de tamanho fixo (512 bytes), que são formadas de uma mensagem com camadas sucessivas de encriptação.
- Essas células, após serem enviadas, são decriptadas por uma chave simétrica em cada nó que passam (processo análogo à descascar uma cebola: a cada nó, uma camada de encriptação é “descascada”, sendo a mensagem resultante retransmitida para o nó seguinte, até chegar ao destino final).

Onion Routing



Onion Routing

- O conteúdo da mensagem, portanto, pode ser visto apenas pelo emissor, pelo destinatário e pelo último nodo (aquele que realiza o último decriptamento)
- Porém, se houver encriptação da mensagem entre o emissor e o destinatário (uso do protocolo SSL/TSL, por exemplo), o último nodo do circuito não terá acesso ao conteúdo da mensagem

Diferenças entre o Tor e o Modelo Original

- O Tor implementa a segunda geração de Onion Routers
- Possui controle de congestionamento, servidores de diretório, verificação de integridade e localização de pontos de rendezvous

Comunicação na Rede Tor

- A rede Tor é uma rede sobreposta, onde cada “roteador cebola” (OR, ou onion router) é executado como um processo em nível de usuário. Cada roteador mantém uma conexão TLS com todos os outros, e cada usuário executa um software local chamado “proxy cebola” (OP, ou onion proxy) para buscar diretórios, estabelecer circuitos e tratar conexões.

Comunicação na Rede Tor

- Cada roteador mantém uma chave de identidade de longo prazo e uma “chave cebola” de curto prazo. A chave de identidade é usada para assinar certificados TLS, para assinar o descritor do roteador (resumo das suas chaves, endereços, largura de banda, política de saída, etc), e por servidores de diretório, para assinar diretórios. A chave cebola é usada para descriptografar solicitações dos usuários para criar um circuito e negociar chaves efêmeras.

Figura


SERVERS
THE CLOUD
AMAZON
WIKIPEDIA
THE WEB SEA
Google
PORN
DEEP WEB
HACKERS
WIKILEAKS
CONTINENTAL
CONTENTS
GOVERNMENT
UNDETECTED
ILLEGAL PORN

Usos

- O Tor foi desenvolvido originalmente para proteger comunicações governamentais. Hoje em dia, ele é usado por milhares de pessoas ao redor do mundo, com as mais diversas finalidades.

Uso na China

- Na China, por exemplo existe um controle muito forte sobre a internet. Alguns conteúdos são bloqueados e existe uma monitoração muito grande. Lá as companhias que fornecem acesso a internet são responsáveis pelo que seus usuários fazem, então as próprias empresas e as pessoas se regulam com medo das consequências legais. Como a rede Tor fornece anonimato, o acesso a rede Tor foi bloqueado.

Usos

- A rede Tor ainda permite que websites e servidores sejam acessados sem que o ip desses servidores seja conhecido, nesse caso esses servidores são acessados por um endereço próprio da rede Tor desde que se tenha uma proxy apropriada.

Vunerabilidade

- O projeto Tor é eficiente contra análise de tráfego e possíveis bisbilhoteiros, porém tem algumas vulnerabilidades. Se um adversário tiver controle sobre o nó de entrada e o de saída de um circuito da rede Tor, então ele consegue identificar quem está falando com quem. O adversário poderia também corromper o tráfego em algum ponto do circuito e ver aonde apareceria esse mesmo padrão.

Vunerabilidade

- A rede Tor não é eficiente contra confirmação de tráfego. Se existir uma suspeita de que alguém está usando Tor para acessar algum destino conhecido, essa suspeita pode ser facilmente confirmada.

Conclusão

- Com o advento da Internet, foi possível interconectar diversos sistemas diferentes, assim como pessoas – através das redes sociais. Porém, o uso dessa ferramenta traz riscos, intrínsecos à computação, à privacidade e a segurança de dados privados.

Conclusão

- Apesar de usar o sistema de roteamento por camadas, ou Onion Routing, a rede ainda é suscetível a ataques (ainda que esses sejam de complexidade maior que ataques comuns a Web), o que gera reflexões sobre a impossibilidade de se construir um sistema totalmente seguro, afim de proteger a privacidade de seu usuário.