
MAC0352 - Redes de Computadores e Sistemas Distribuídos

Daniel Macêdo Batista

IME - USP, 20 de Maio de 2021

Roteiro

Programação com
sockets UDP

Anonimização na
Internet – Tor

Programação com sockets UDP

Anonimização na Internet – Tor

► Programação com
sockets UDP

Anonimização na
Internet – Tor

Programação com sockets UDP

Cliente de echo

Programação com
sockets UDP

Anonimização na
Internet – Tor

- Envia linhas para o servidor
- Recebe as linhas do servidor e imprime na saída padrão
- Pode conectar pelo nome ou pelo IP (função
`gethostbyname`)
- Envia o primeiro sendto

Servidor de echo

Programação com
sockets UDP

Anonimização na
Internet – Tor

- Recebe linhas enviadas pelos clientes
- Devolve as linhas para os clientes e imprime na saída padrão

Programação com
sockets UDP

▷ Anonimização na
Internet – Tor

Anonimização na Internet – Tor

Informações “particulares” na Internet

Programação com
sockets UDP

Anonimização na
Internet – Tor

- Endereço IP de origem, porta de origem
- Endereço IP de destino, porta de destino
- Serviço sendo acessado (no caso de HTTP, a URL)
- Momento em que o acesso foi realizado

Por que e como anonimizar?

Programação com
sockets UDP

Anonimização na
Internet – Tor

- **Um sniffer na rede local da origem ou no destino consegue as informações de origem, destino e momento do acesso**
- No caso específico de HTTP, o HTTPS já criptografa a URL mas outras informações continuam visíveis
- Com o uso de proxy, o momento do acesso pode ser escondido mas e se o administrador do proxy não for confiável?
 - O proxy também ocultaria o endereço IP do remetente se um sniffer fosse usado na rede local do destino
- Endereços IPs precisam ser mantidos porque são eles que são usados para rotear os pacotes na Internet

Tor

Programação com
sockets UDP

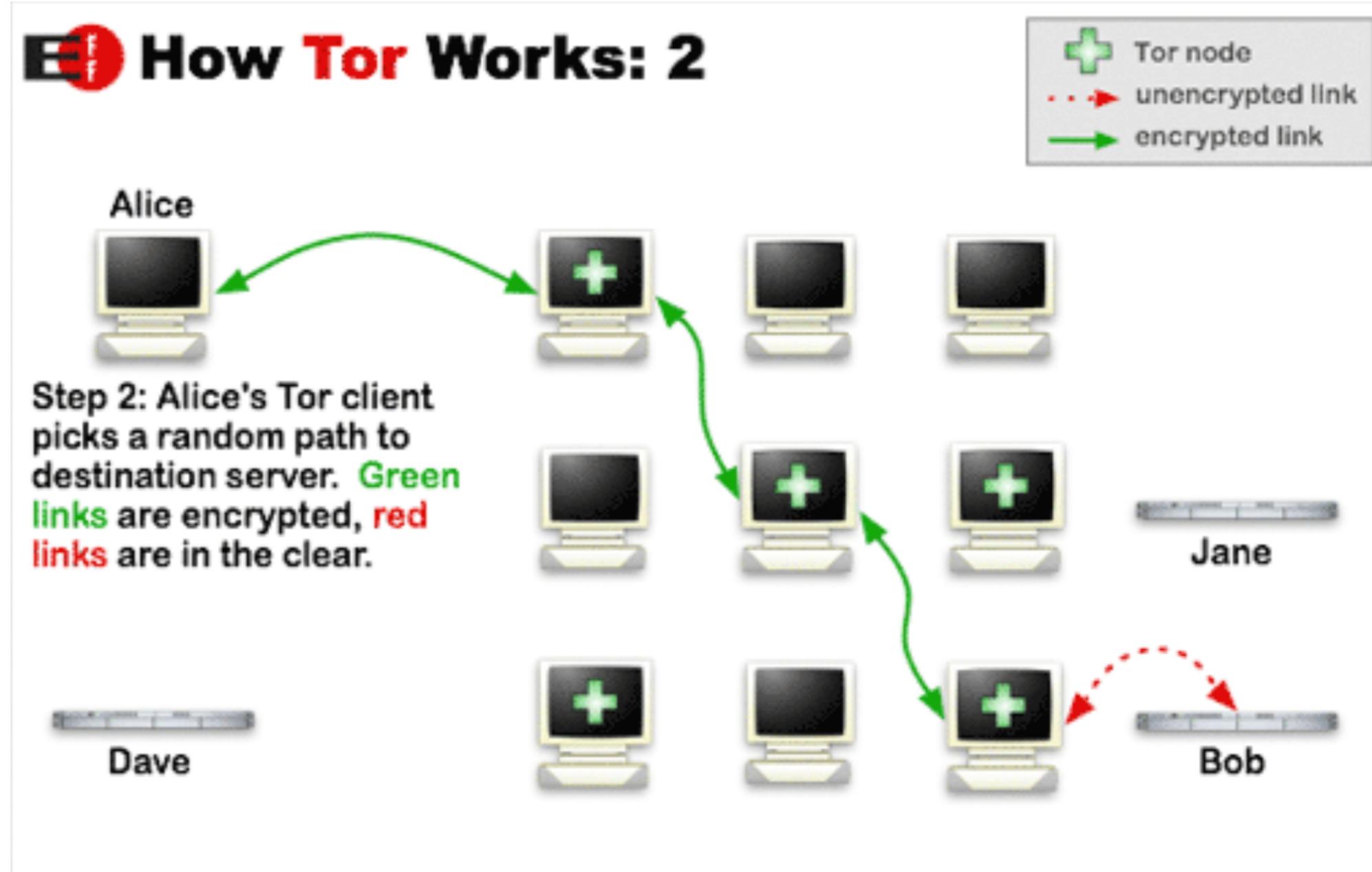
Anonimização na
Internet – Tor

- Tor (The Onion Router)
- O objetivo é permitir comunicações anônimas pela Internet
 - Usa criptografia na camada de aplicação e uma rede de relays que repassam as mensagens para diversos hosts antes de chegar no destino
 - A referência a “cebola” é porque cada acesso a um host é criptografado com a chave pública daquele host, levando à analogia de uma cebola por causa das diversas camadas
- Ainda é possível saber que o Tor está sendo usado em alguma ponta da comunicação e quando está sendo usado mas não é possível descobrir quem são as duas pontas da conexão.

Tor

Programação com
sockets UDP

Anonimização na
Internet – Tor



<https://2019.www.torproject.org/about/overview.html.en>