Segurança e Privacidade para Iniciantes

Jéssica Carneiro (UFMG)

Quem sou eu?

- Bacharel em Ciência da Computação pela UFMG (2013-2018)
- Bolsista intercambista pelo Ciência sem Fronteiras (2015-2016)
- Mestranda em Ciência da Computação na UFMG (2018-2020)
- Trabalho com pesquisa desde 2016 na área de segurança digital
  - Internet das Coisas
  - Autenticação Federada
  - Criptografia pós-quântica

Segurança? Privacidade?

Segurança! Privacidade!

Por que precisamos falar sobre isso?

- **2013**: Target (varejista EUA) 110 milhões de usuários (cartões de crédito/débito e informações dos clientes expostas)
- **2014**: eBay 145 milhões de contas de usuários expostas
- **2016**: Yahoo! 1 bilhão de contas de usuários expostas
- **2017**: WannaCry afetou mais de 150 países (incluindo o Brasil)

O maior problema?

O que é segurança digital, afinal?

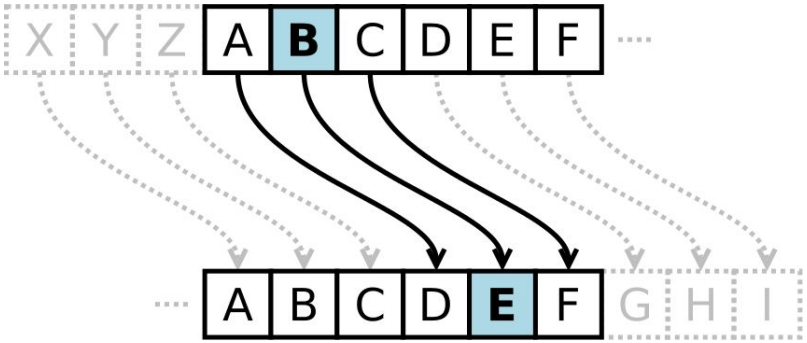
De acordo com a Wikipedia:

- Consiste na NÃO violação da:
  - Confidencialidade
  - Integridade
  - Disponibilidade
  - Autenticidade
- de documentos e dados pessoais

WIKIPEDIA
The Free Encyclopedia

Confidencialidade

- Evitar que pessoas não autorizadas tenham acesso a um dado ou informação
- É uma necessidade humana muito antiga
  - Exércitos precisam trocar informações
    - Cifra de César



Integridade

- Propriedade que garante que um dado ou informação não foi adulterado de uma forma inapropriada
- Exemplo: telefone sem fio

Disponibilidade

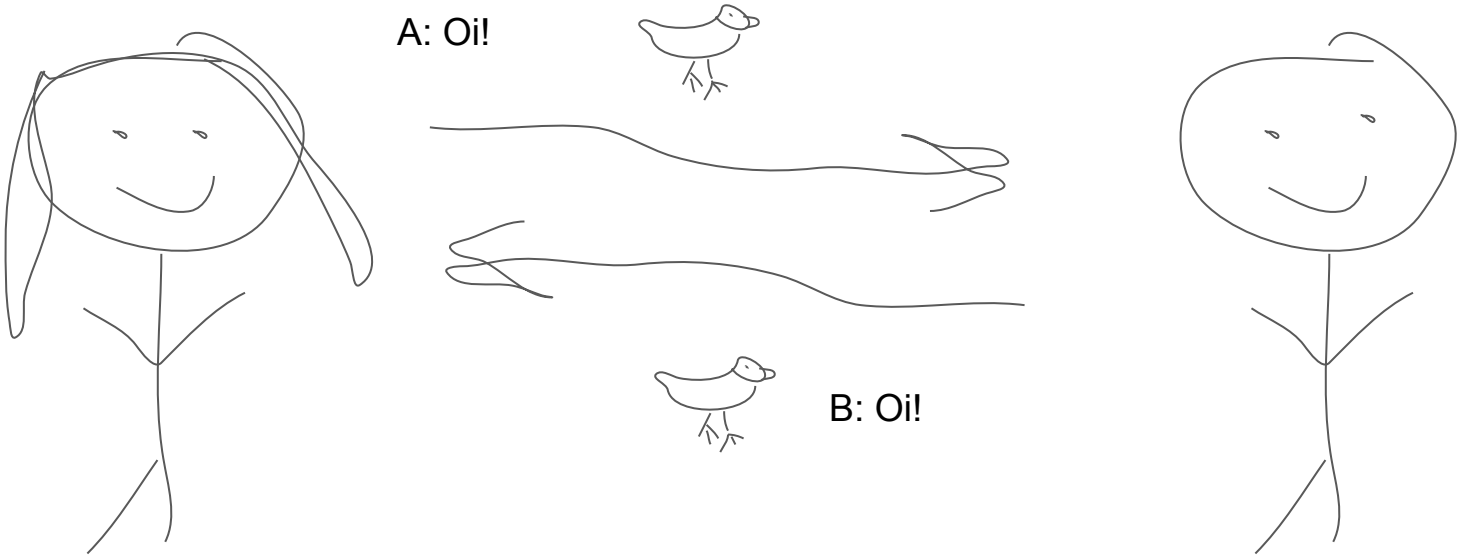
- Propriedade que garante que uma informação esteja disponível e possa ser modificada em tempo hábil por indivíduos autorizados
- Exemplos: WannaCry

Autenticidade (ou Autenticação)

- É a habilidade de determinar que mensagens, informações, requisições emitidas por um indivíduo ou sistema são genuínas.
- Não repúdio: um indivíduo não pode negar a autoria de uma mensagem

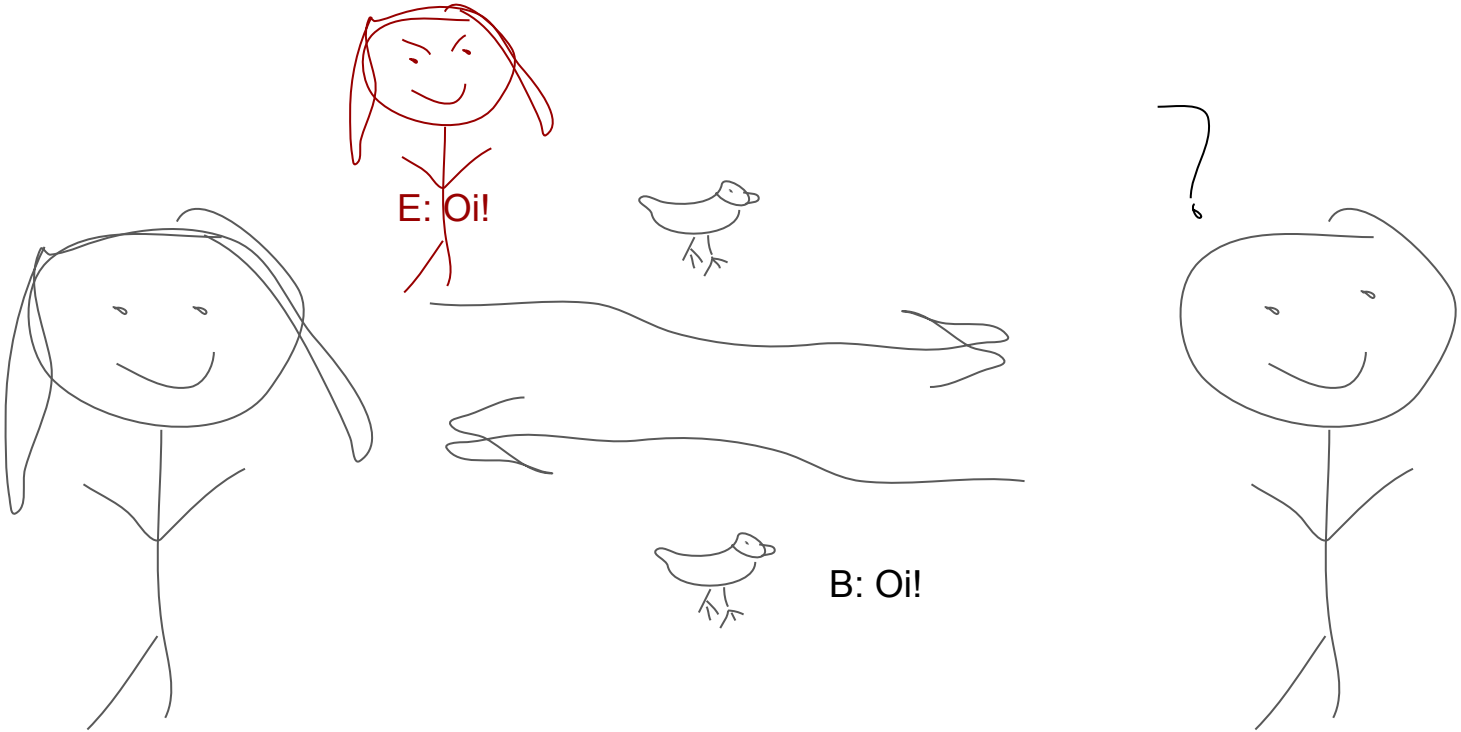
Vamos falar de criptografia… e pombos!

- Alice e Bob querem conversar… e usam pombos



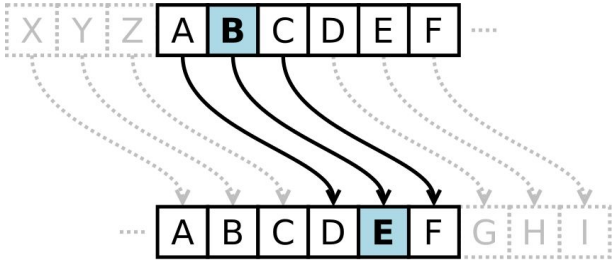
Vamos falar de criptografia… e pombos!

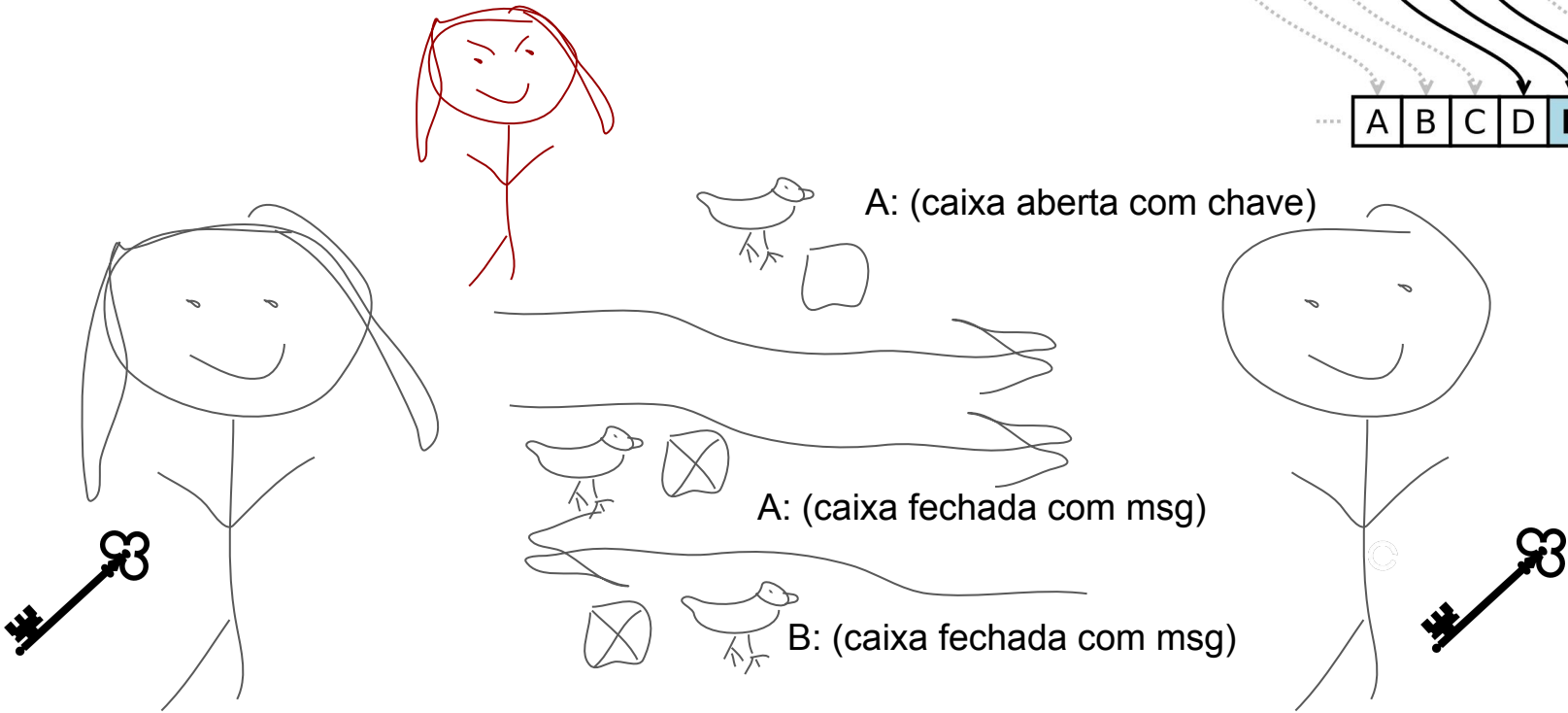
- Alice e Bob querem conversar… e usam pombos



Vamos falar de criptografia… e pombos!

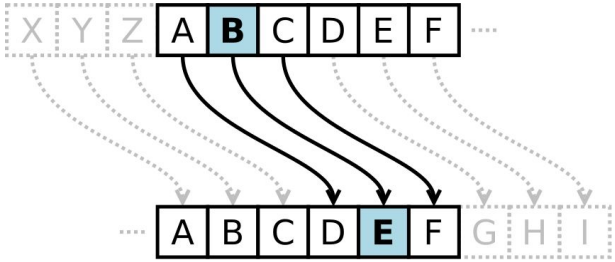
- Alice e Bob querem conversar… e usam pombos

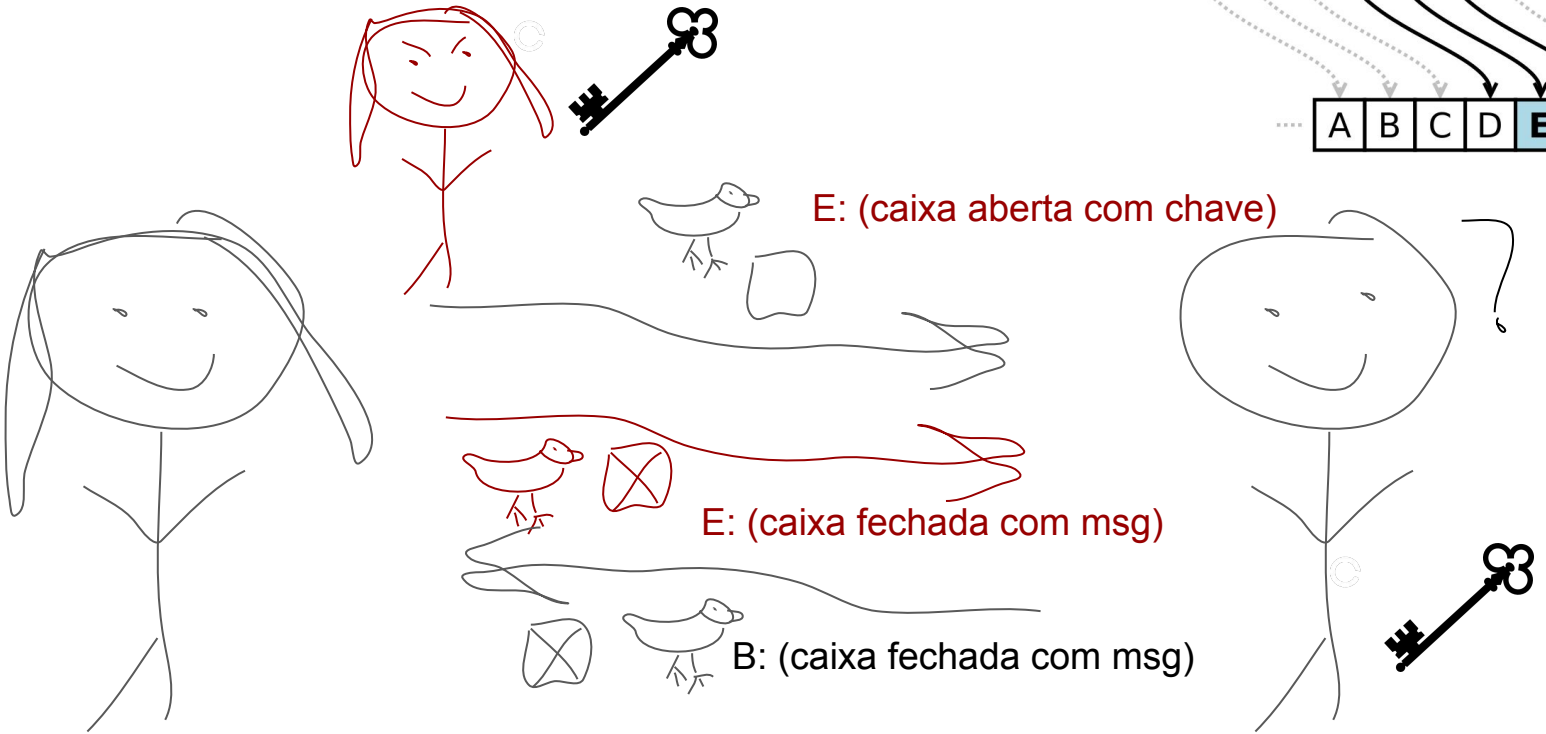




Vamos falar de criptografia… e pombos!

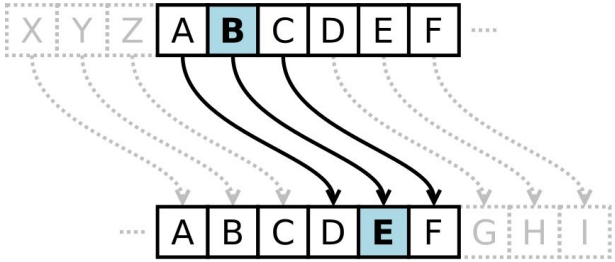
- Alice e Bob querem conversar… e usam pombos

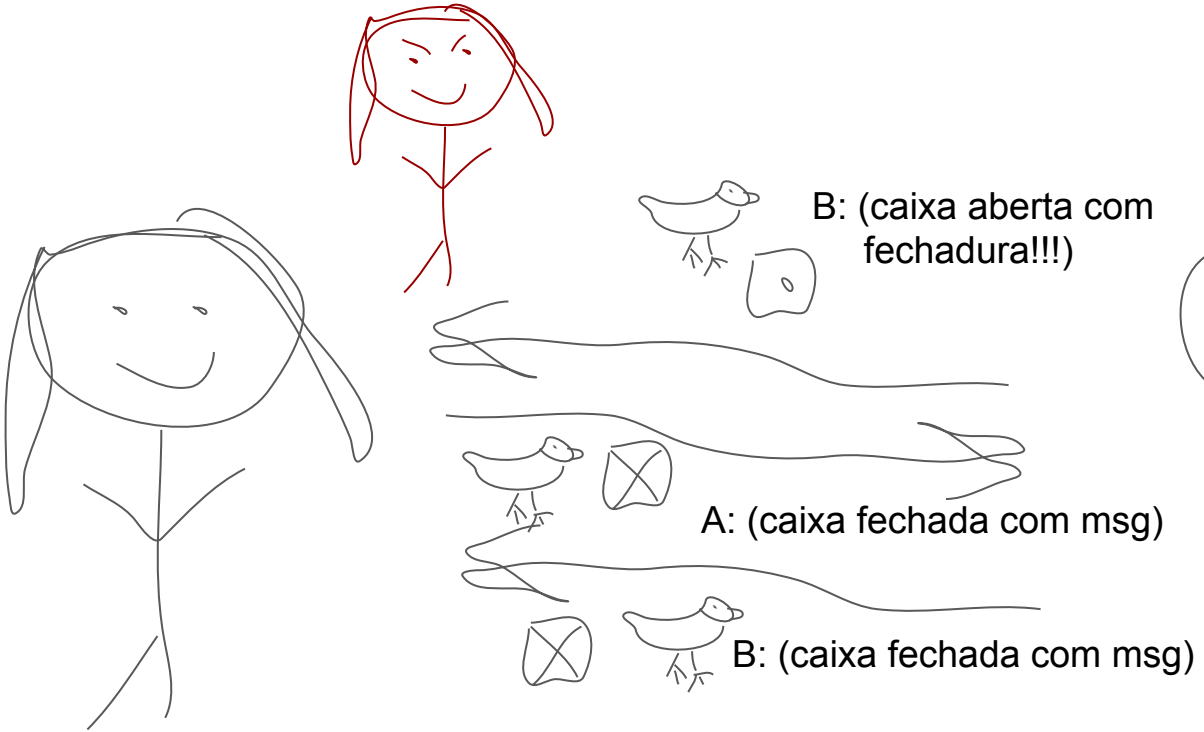




Vamos falar de criptografia… e pombos!

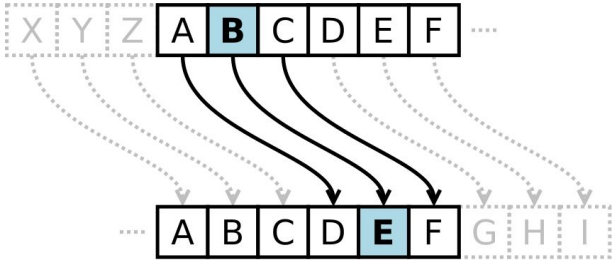
- Alice e Bob querem conversar… e usam pombos

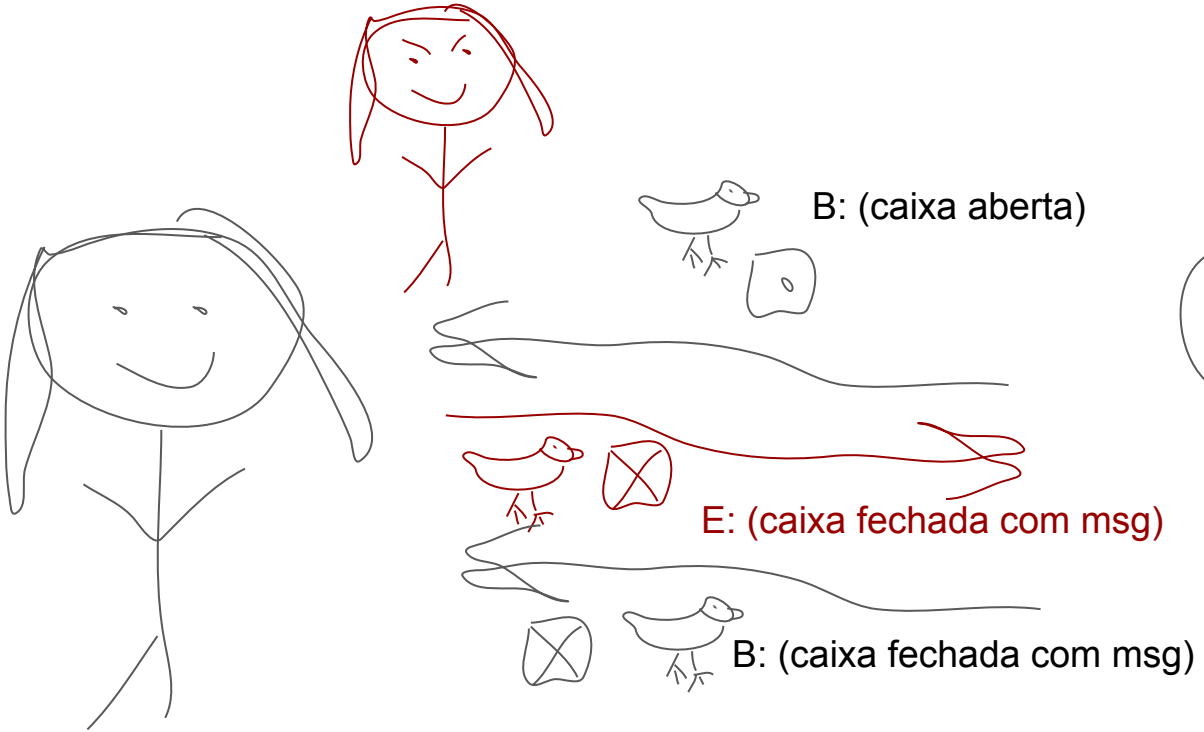


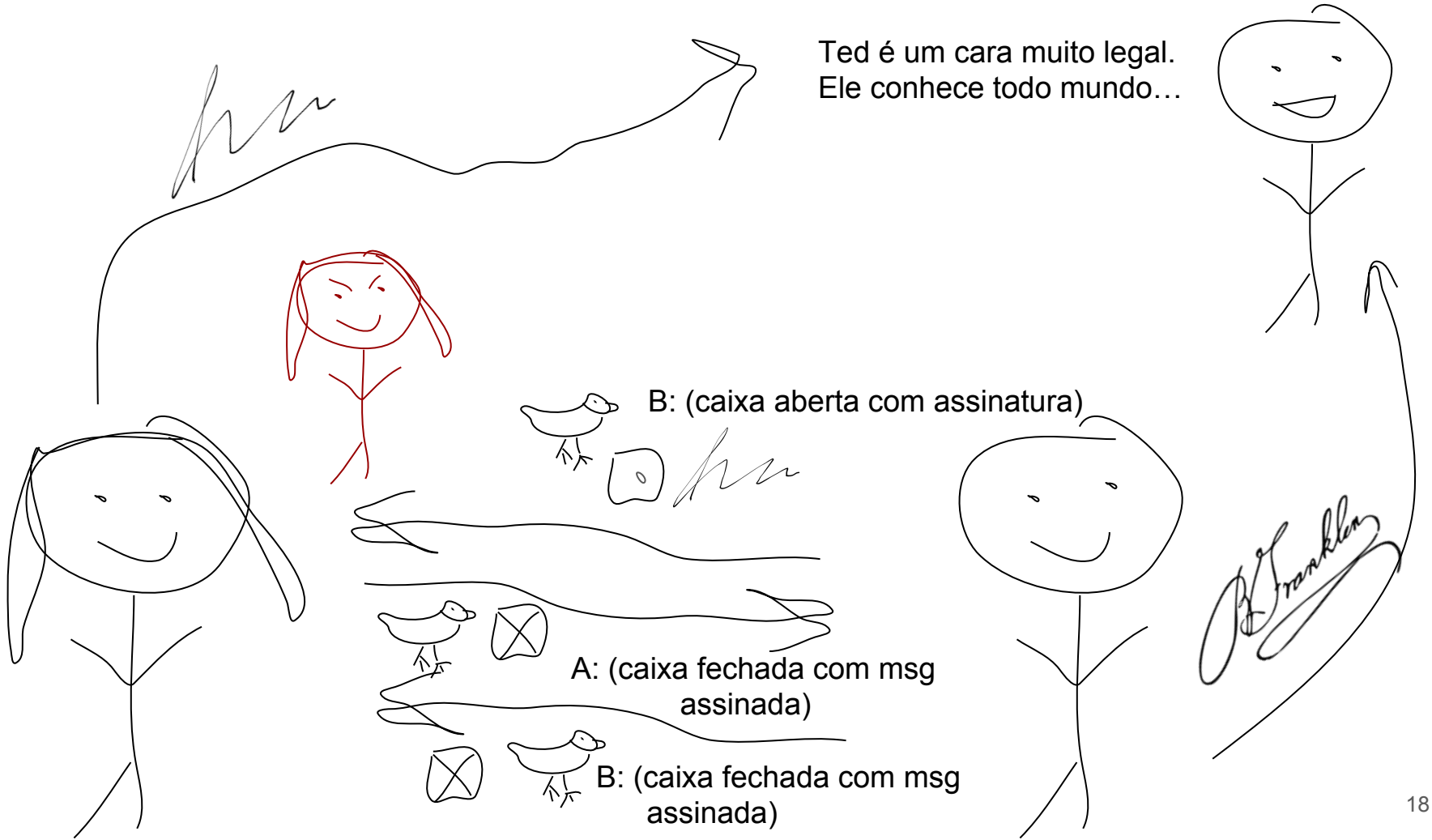


Vamos falar de criptografia… e pombos!

- Alice e Bob querem conversar… e usam pombos





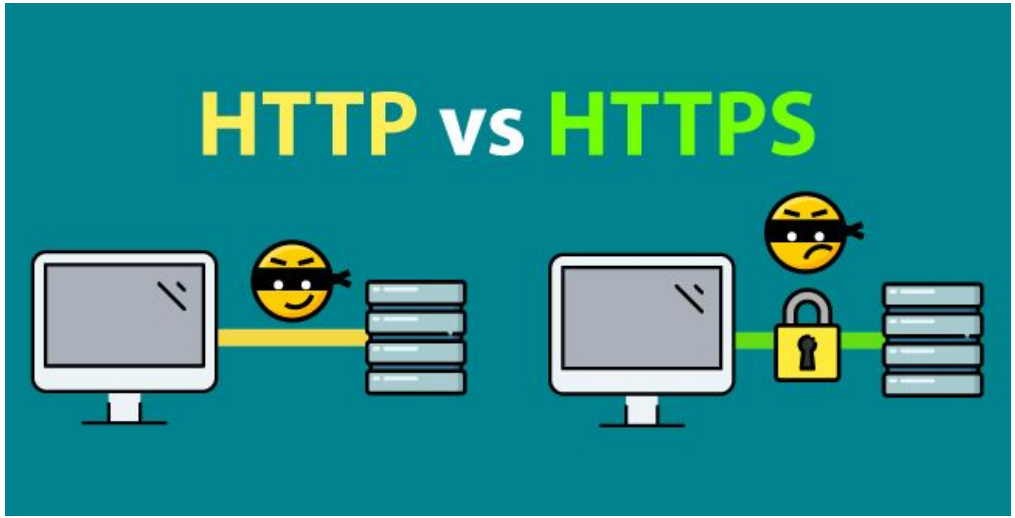

Ted é um cara muito legal.
Ele conhece todo mundo…
B: (caixa aberta com assinatura)
A: (caixa fechada com msg assinada)
B: (caixa fechada com msg assinada)

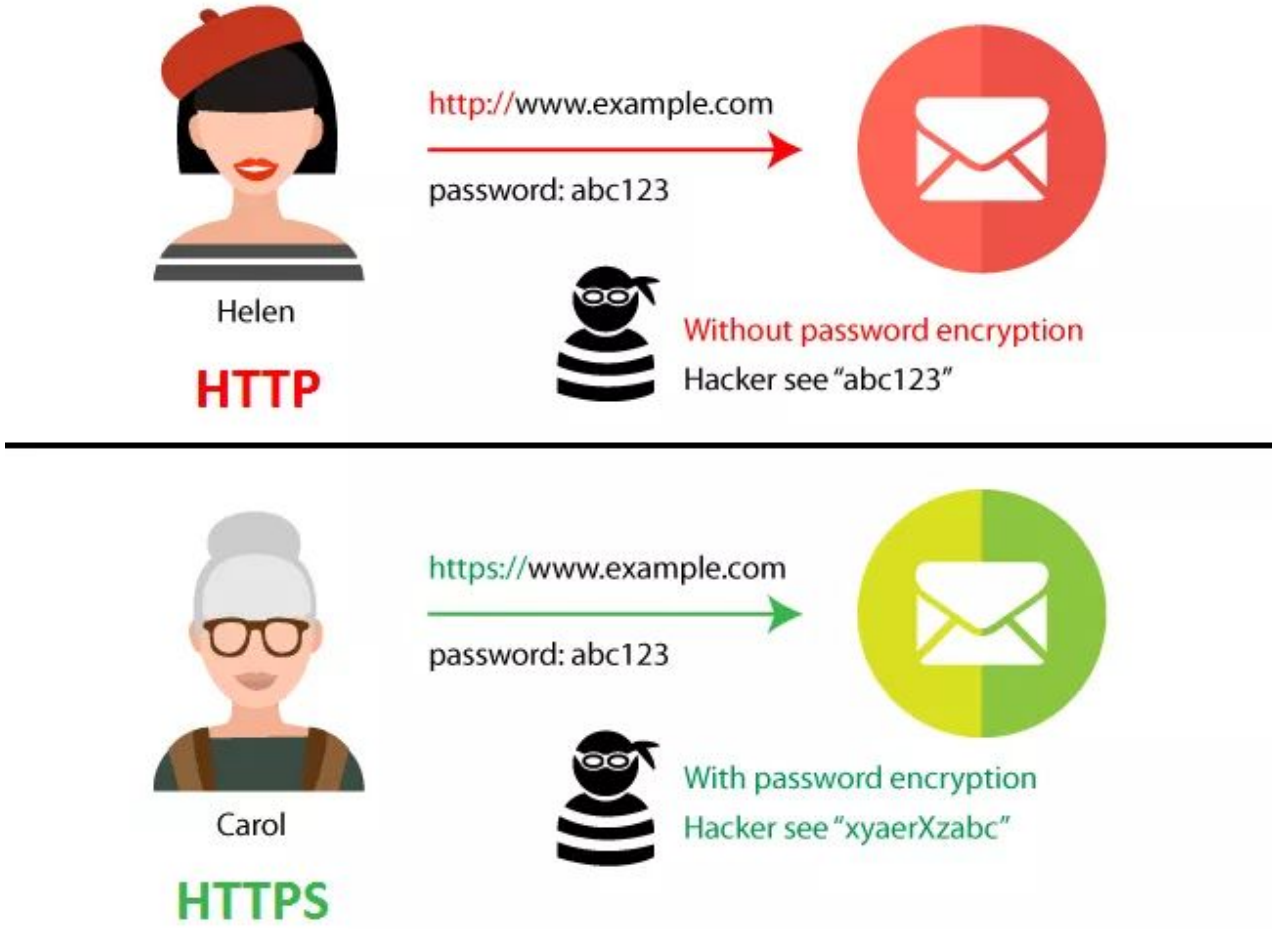
Vamos falar de criptografia… e pombos!

- Alice e Bob querem conversar… e usam pombos com chaves públicas e usando certificados!
  - Garantem autenticação
  - Garantem confidencialidade
  - Garantem integridade (se mensagem for alterada, não fará sentido algum!)

Como garantir essas propriedades?

- Na World Wide Web (WWW):
  - HTTPS: protocolo que estabelece uma comunicação segura entre o navegador do usuário e o site com o qual está se comunicando mesmo se não habilitada
    - HTTPS Everywhere: https://www.eff.org/https-everywhere




http://www.example.com
password: abc123
Helen
HTTP
Without password encryption
Hacker see "abc123"
https://www.example.com
password: abc123
Carol
HTTPS
With password encryption
Hacker see "xyaerXzabc"

Como garantir essas propriedades?

- Senhas:
  - NÃO utilizar a mesma senha em TODOS os sites/serviços
    - Gerenciadores de senhas:
      - LastPass https://www.lastpass.com/pt
      - 1Password https://1password.com/
  - Não utilizar senhas óbvias
  - Utilize senhas grandes (> 8 caracteres)
  - Verifique se seus dados foram expostos: https://haveibeenpwned.com/
  - Autenticação de 2 fatores
    - Facebook
    - Google
    - Twitter
    - Apple
    - SMS

Rank	2011[4]	2012[5]	2013[6]	2014[7]	2015[8]	2016[3]	2017[9]
1	password	password	123456	123456	123456	123456	123456
2	123456	123456	password	password	password	password	password
3	12345678	12345678	12345678	12345	12345678	12345	12345678
4	qwerty	abc123	qwerty	12345678	qwerty	12345678	qwerty
5	abc123	qwerty	abc123	qwerty	12345	football	12345
6	monkey	monkey	123456789	123456789	123456789	qwerty	123456789
7	1234567	letmein	111111	1234	football	1234567890	letmein
8	letmein	dragon	1234567	baseball	1234	1234567	1234567
9	trustno1	111111	iloveyou	dragon	1234567	princess	football
10	dragon	baseball	adobe123[a]	football	baseball	1234	iloveyou

Como garantir essas propriedades?

- SEMPRE ATUALIZE SEU SISTEMA OPERACIONAL (seja no computador desktop, smartphone, laptop, tablet, …)
  - Aplicativos também :D
- Correções para falhas e vulnerabilidades são feitas periodicamente pelas empresas ou sempre que um problema for descoberto

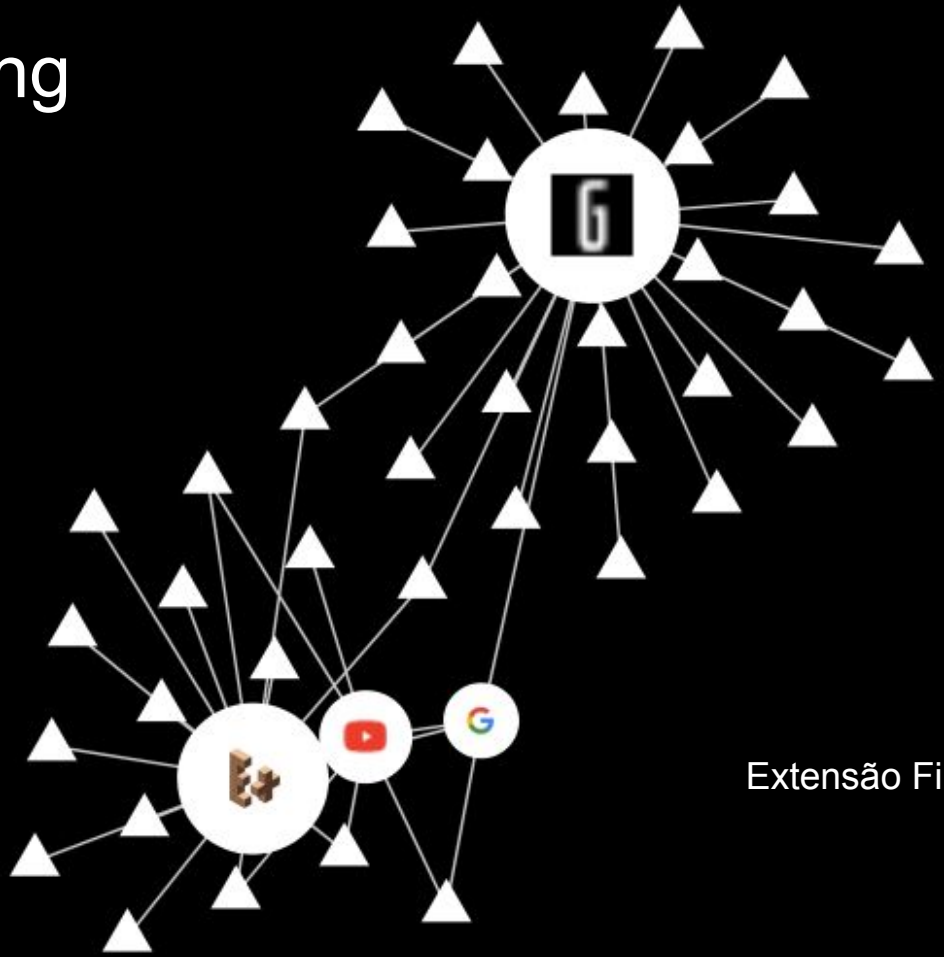
Privacidade

- Da Wikipedia: É o direito à reserva de informações pessoais e da própria vida pessoal
- Existe SIM uma sobreposição de privacidade e segurança

Privacidade

- Conveniência x Privacidade
- Marketing direcionado x Marketing neutro
  - Seleção baseada no perfil do usuário
- Bolha da Internet
  - Influências
  - Reforço de ideologias
  - Preferências

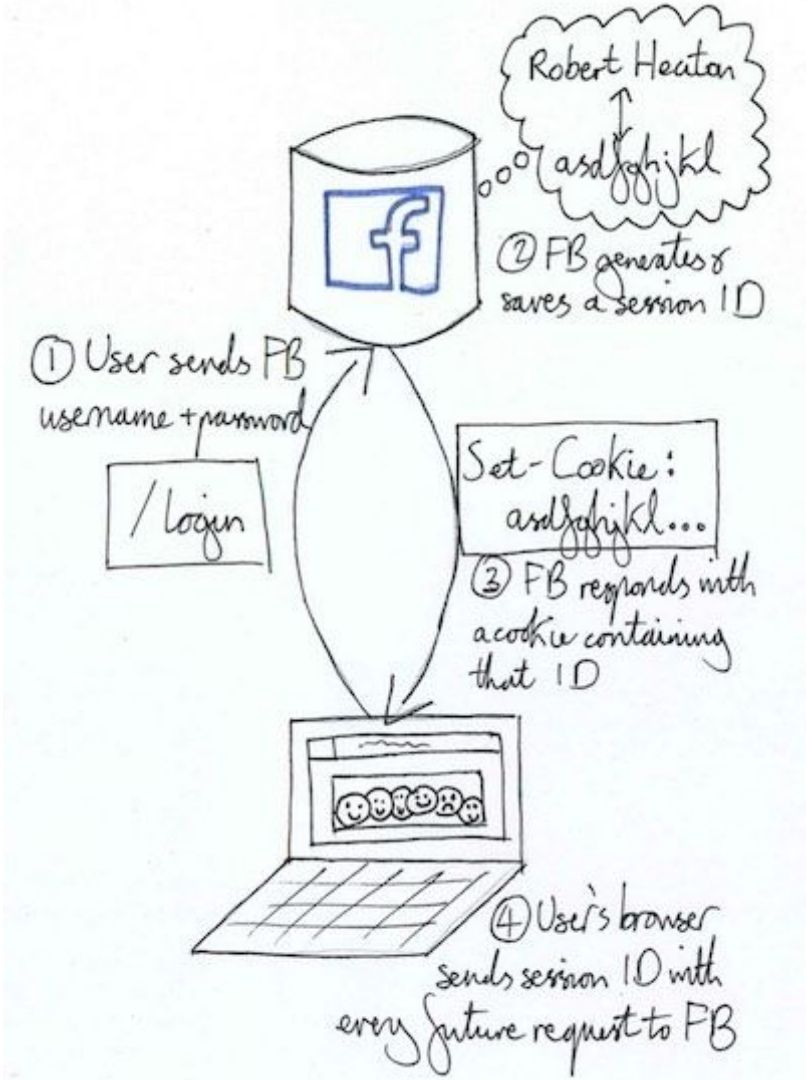
Online Tracking

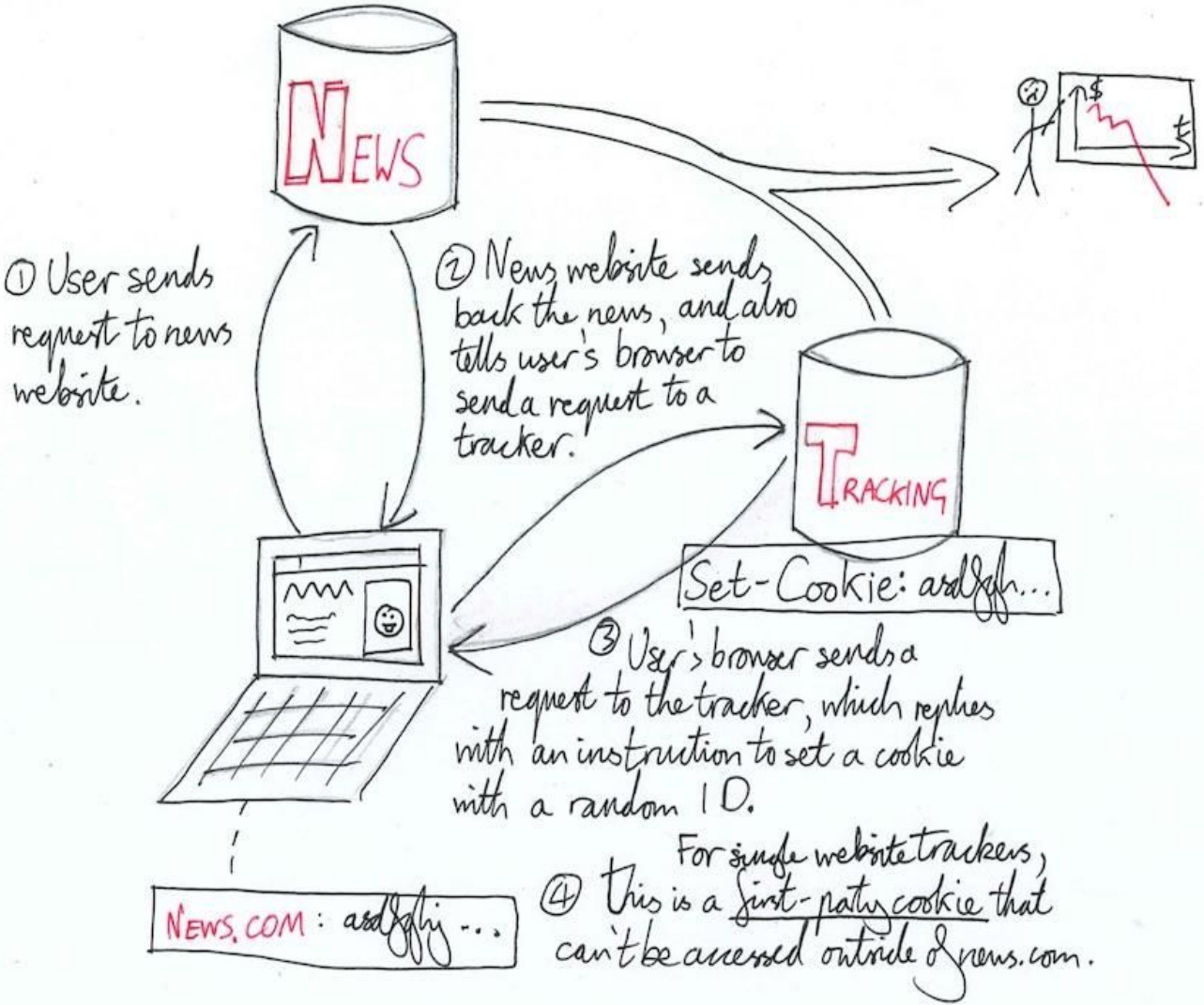


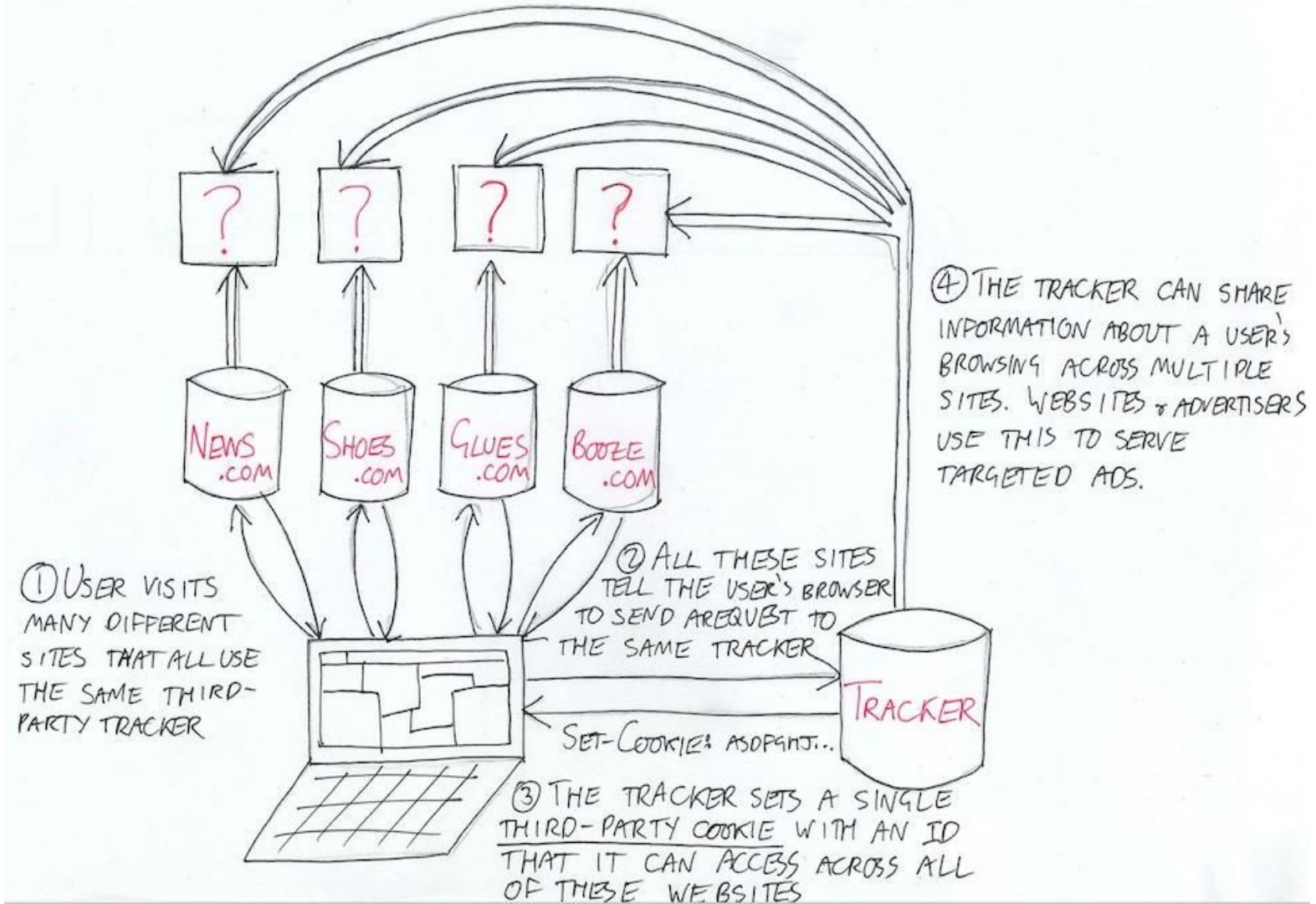
Extensão Firefox Lightbeam

Vamos falar sobre cookies...

- Arquivo no computador do usuário
  - Criado pelo navegador (Chrome, Firefox, Safari, Opera....)
  - Armazena ID da sessão (logado/não logado)
  - Informações de preferência do usuário
  - Serve para tracking


Robert Heaton
asdfghjkl
② FB generates & saves a session ID
① User sends FB username + password
/login
Set-Cookie: asdfghjkl...
③ FB responds with a cookie containing that ID
④ User's browser sends session ID with every future request to FB


NEWS
$
①User sends request to news website.
②News website sends back the news, and also tells user's browser to send a request to a tracker.
TRACKING
Set-Cookie: asdfgh...
③User's browser sends a request to the tracker, which replies with an instruction to set a cookie with a random ID.
NEWS.COM : asdfghj...
④This is a first-party cookie that can't be accessed outside of news.com.
For single website trackers,

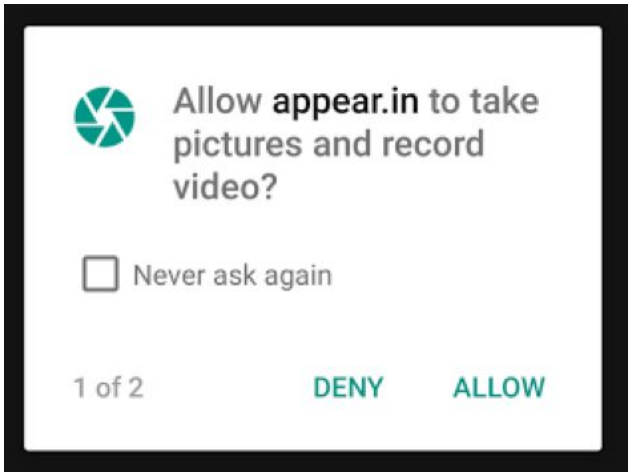

?
?
?
?
NEWS .COM
SHOES .COM
GLUES .COM
BOOZE .COM
TRACKER
SET-COOKIE: ASDFGHJ..
④ THE TRACKER CAN SHARE INFORMATION ABOUT A USER'S BROWSING ACROSS MULTIPLE SITES. WEBSITES & ADVERTISERS USE THIS TO SERVE TARGETED ADS.
① USER VISITS MANY DIFFERENT SITES THAT ALL USE THE SAME THIRD-PARTY TRACKER
② ALL THESE SITES TELL THE USER'S BROWSER TO SEND A REQUEST TO THE SAME TRACKER
③ THE TRACKER SETS A SINGLE THIRD-PARTY COOKIE WITH AN ID THAT IT CAN ACCESS ACROSS ALL OF THESE WEBSITES

Como proteger sua privacidade?

- Ativar “não me seguir” nas preferências do seu navegador (padrão)
  - Pode ser suficiente se você não é paranoica
- Muitos *trackers* estão evoluindo (sem usar cookies)
- Recomendação: instalar um adblocker
  - Remover/alterar conteúdo de publicidade de uma página
  - AdBlock https://getadblock.com/
- Recomendação: pesquisas “sensíveis”
  - Use um buscador que não te entregará (ex.: DuckDuckGo!)

Como proteger sua privacidade?

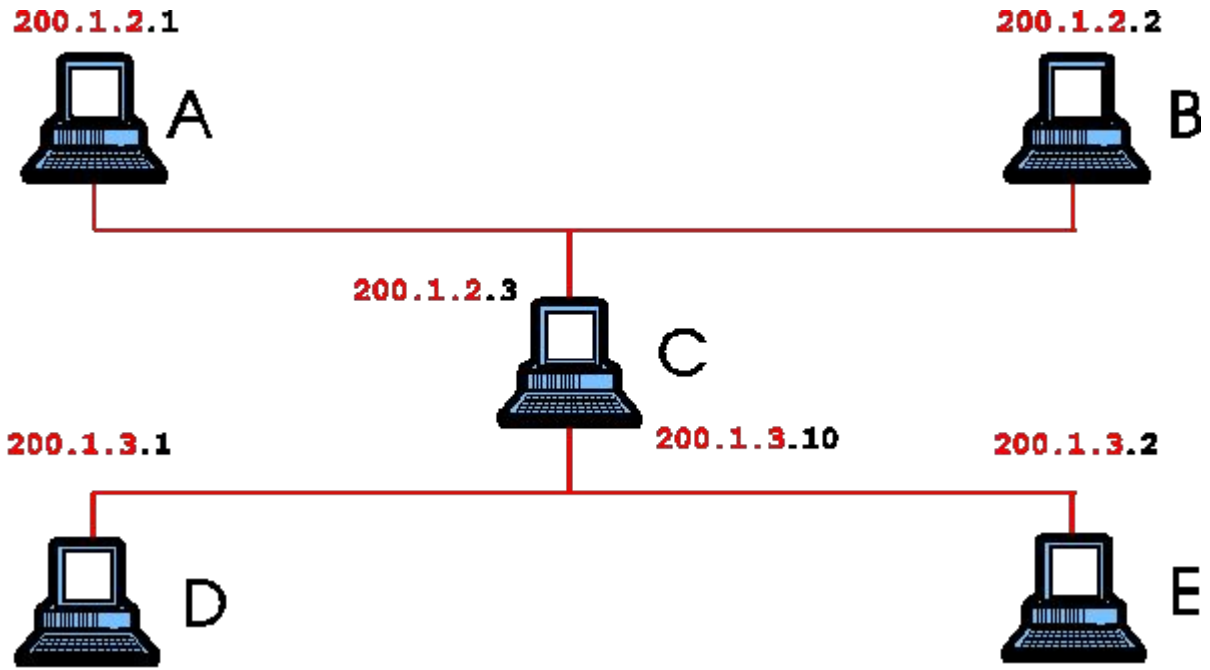
- Cuidado com o que compartilha com serviços terceiros
  - Login via Facebook, Google, Twitter… usa informações e possui permissões
    - E-mail, nome, idade, local
    - Postar na sua linha do tempo, ler e-mails, enviar mensagem
  - Aplicativos para smartphones também pode pedir informações e permissões
    - Uso de câmera, microfone, localização, ...



Deep Web

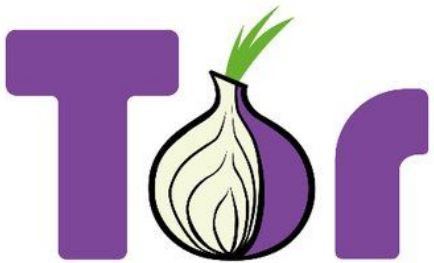
- Web não indexada por buscadores (ex.: Google)
- Navegador próprio (Chrome não vai te levar a lugar algum, use o Tor)
- Endereços “esquisitos” (zqktlwi4fecvo6ri.onion)
- Conhecida por abrigar criminosos (Road Silk 2013, FBI)
- Importante para jornalistas, pessoas em países de regime totalitário, exilados políticos (ex.: Edward Snowden)

Protocolo IP

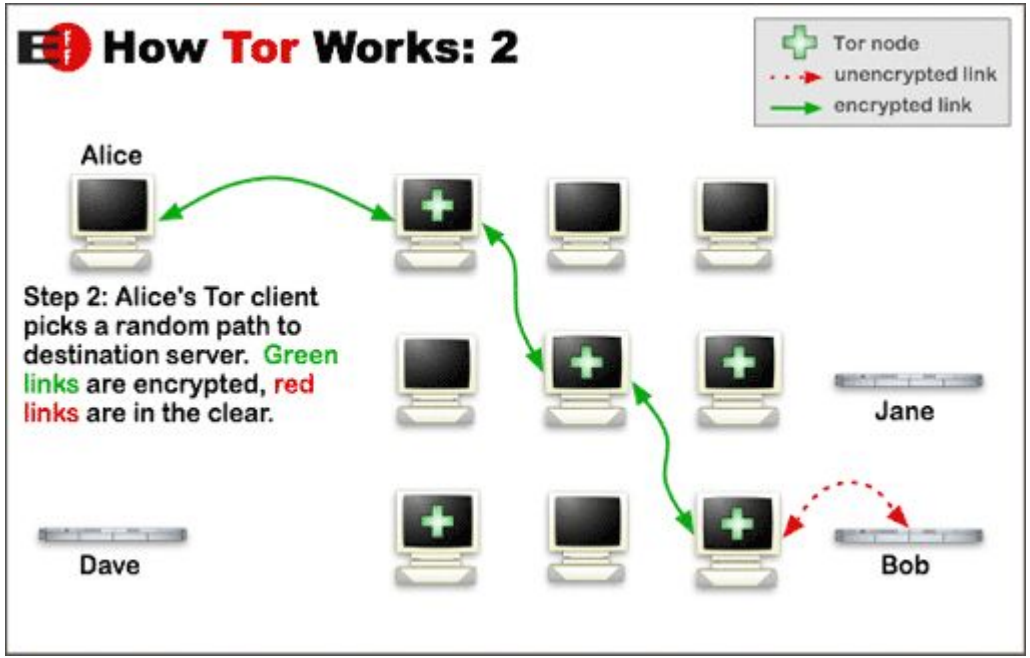


Projeto Tor (“The Onion Router”)

- Navegador baseado no Firefox
  - Livre, gratuito, código aberto, anônimo
- Permite que usuário fique livre de *trackers*
  - Navegador não revela localização do usuário
  - Roteadores na rota da mensagem não conhecem o caminho



Projeto Tor (“The Onion Router”)



Engenharia Social

- Um dos maiores desafios…
- Conseguir informações através de pessoas
  - Como impedir?
  - Como garantir que seu negócio/sistema não possui falhas humanas?
- Exemplo: “pen drive perdido” (no seriado Mr. Robot)

Obrigada!

Dúvidas?

Contato: jessicacarneiro@dcc.ufmg.br

Twitter/Facebook/Instagram/Snapchat/ ...: /**jessicacarneir0**