Útoky na Tor

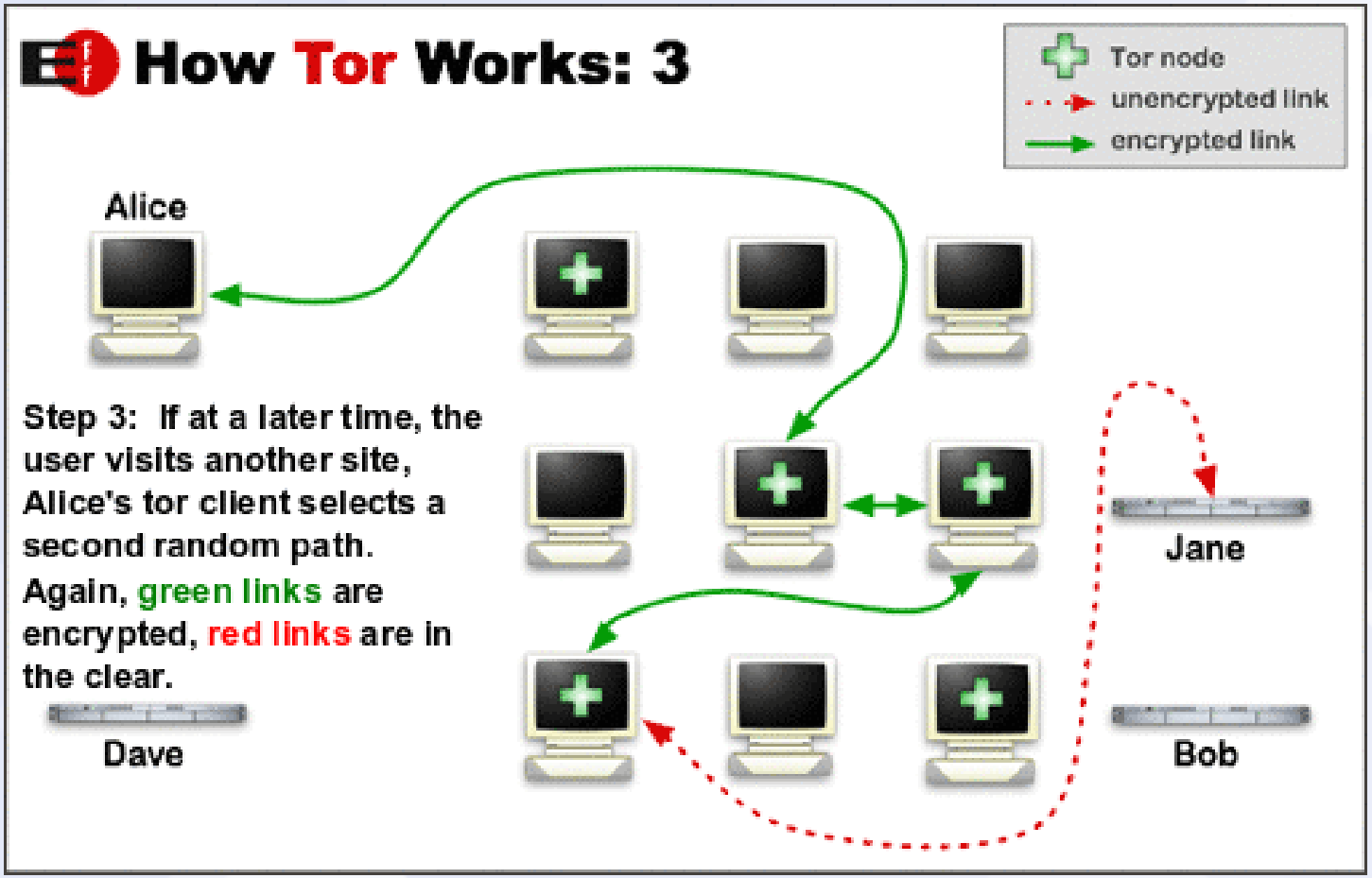
především ty víc praktické

hiviah • hiviah@torproject.org • 1.6.2016

Tor není určen na...

- ochranu proti „global passive adversary“
- sanitizování metadat uvnitř protokolů
- „kryptografie se typicke neprolamuje, ale obchází“

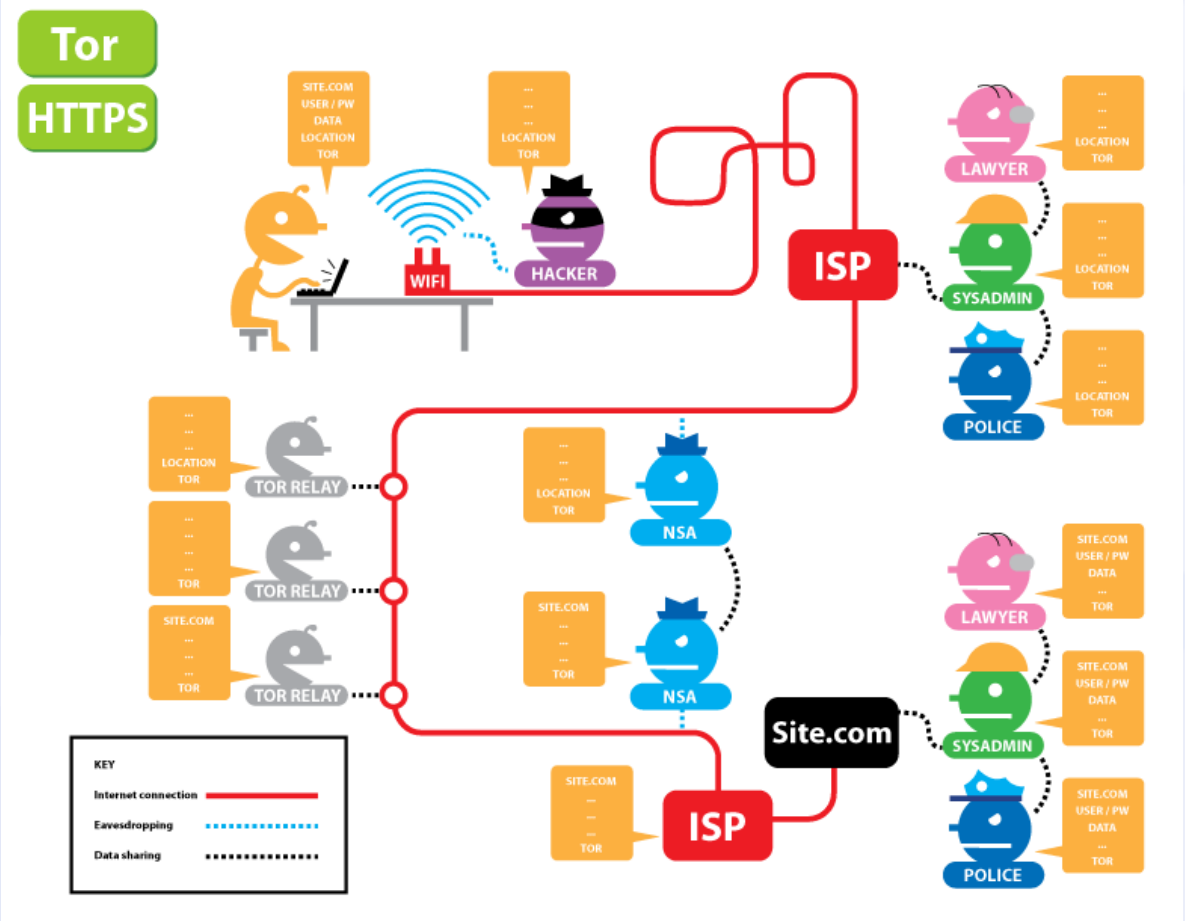
Tor


How Tor Works: 3
Tor node
unencrypted link
encrypted link
Alice
Step 3: If at a later time, the user visits another site, Alice's tor client selects a second random path.
Again, green links are encrypted, red links are in the clear.
Dave
Jane
Bob

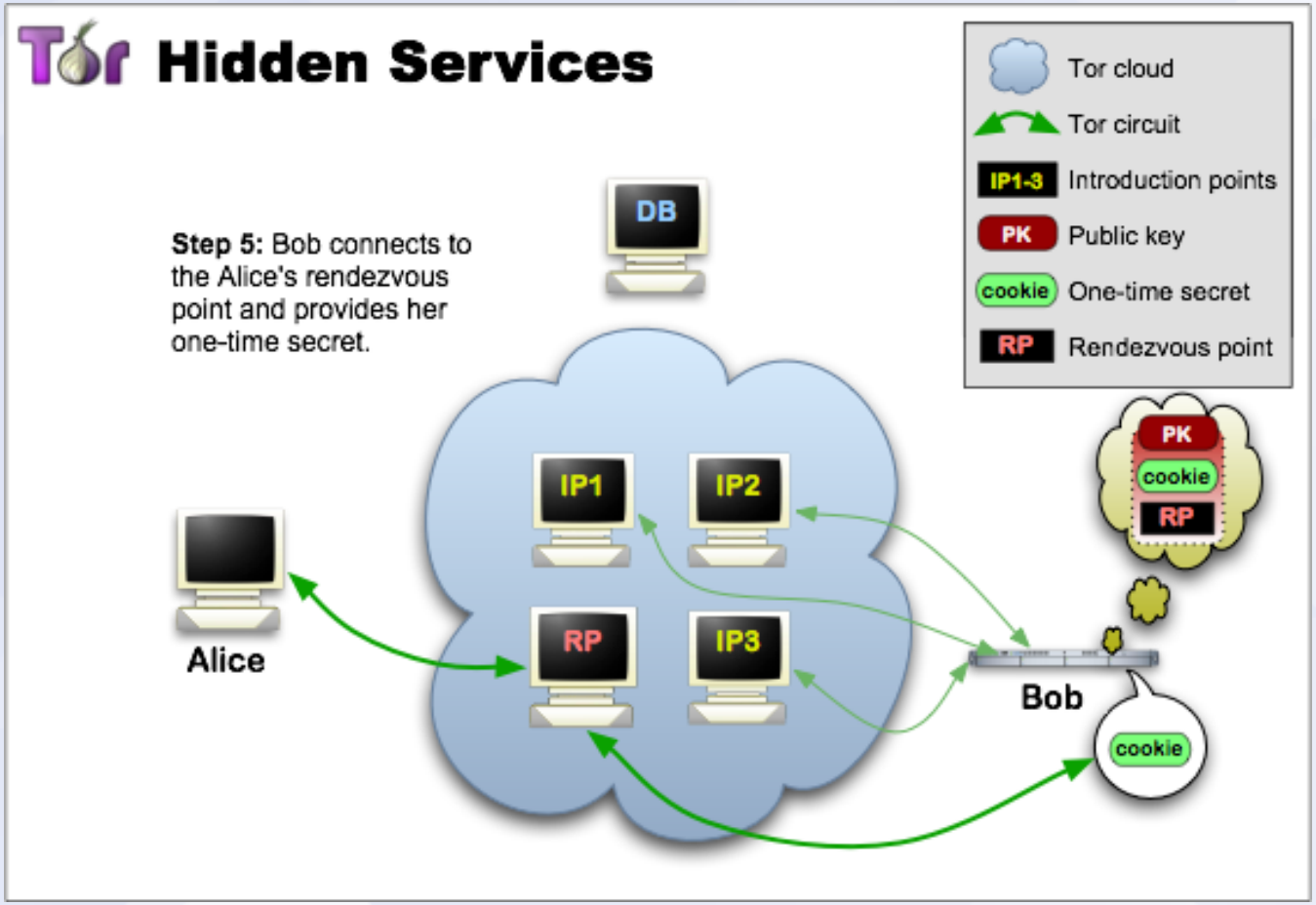
Stavění cesty přes Tor

- „circuit“ je proxy přes 3 Tor relay nody
  - první je „entry guard“
  - druhý je „middle relay“
  - třetí je „exit relay“
- packet v Tor síte se jmenuje „cell“
- „circuit“ má omezenou časovou životnost
- hidden services (HS) mají víc nodů v cestě mezi klientem a HS

Tor + https


Tor
HTTPS
SITE.COM
USER / PW
DATA
LOCATION
TOR
LOCATION
TOR
WIFI
HACKER
ISP
LAWYER
SYSADMIN
POLICE
LOCATION
TOR
TOR RELAY
TOR RELAY
TOR RELAY
NSA
NSA
SITE.COM
USER / PW
DATA
TOR
Site.com
ISP
KEY
Internet connection
Eavesdropping
Data sharing

Tor hidden services



Analýza toku sítě

- největší „třída“ útoků
- nemá za cíl dešifrovat obsah komunikace
  - ale kdo s kým kdy komunikoval
- může se to zdát jako slabé
  - je to předvoj k jiným útokům
- dva hlavní typy útoků
  - traffic correlation
  - traffic confirmation

Traffic correlation

- Tor je nízkolatenční síť
- když se začne spojení z jednoho konce, za pár vteřin se objeví na jiném konci
- teoreticky „global passive adversary“ umí korelovat časy pozorováním všech relayů
  - obrana proti GPA není cílem Toru
  - organizace typu NSA nebo EU direktiva „data retention“ jsou příkladem GPA

Traffic correlation (2)

- korelovat lze různé metriky
  - čas kdy pakety dorazily
  - velikost paketů, bursty, směr komunikace
  - vzory v nahrávaní stránek
- obecně velmi těžký
- pořád neví o čem se baví, jen „kdo s kým kdy“

Traffic correlation (3)

- bylo mnoho akademických pokusů
  - The Sniper Attack: Anonymously Deanonymizing and Disabling the Tor Network
  - Circuit Fingerprinting Attack: Passive Deanonymization of Tor
  - Touching from a Distance: Website Fingerprinting Attacks and Defenses
- velmi teoretické útoky

Obrana proti traffic correlation

- časový fingerprinting
  - vkládat náhodné zpoždení
  - volitené u obfs4, ScrambleSuit
  - musí být velké ⇒ horší použitelnost
- fingerprinting velikostí a směru paketů
  - různé typy adaptivního paddingu
    - WTF-PAD, CS-BuFlo, Tamaraw
  - v budoucích verzích obfsproxy (obfs5)

Traffic confirmation

- traffic correlation umí zjistit „kdo s kým kdy“
  - ale ne obsah komunikace
- traffic confirmation umí potvrdit podezření, že Alice komunikuje s Bobem
  - slabší než traffic correlation, protože nejprve musíte mít podezřelého
- trochu jak traffic correlation, ale víte, že musíte zkontrolovat jen logy ISP Alice a logy serveru Boba

Traffic confirmation (2)

- příklad: vidíte, že kolem času 20:03 odešly od Alice 8 paketů velikosti cca 4 kB
- na serveru Boba o pár sekund přišlo zhruba stejné množtví paketů zhruba stejné velikosti
- někdy může být hodně „netechnické“, jako vytrhnutí ethernetového kabelu ze switche (případ Sabu)

Analýza tunelovaného protokolu

- bittorrent je typický příklad protokolu, který není dobré používat s Tor-em
  - uvnitř protokolu se posílá reálná IP
- zdaleka není jediný takový
- Tor se nemůže tomuto magicky bránit, uživatel musí vědet, co netunelovat

Tagging attack

- pokus označit si paket na začátku a pak ho poznat
- tohle normálně vůbec nefunguje
  - každý relay rozbalí packet, „odloupe“ onion vrstvu a pošle dál
- v AES-CTR jdou teoreticky flipováním bitů ciphertextu měnit bity plaintextu
  - už dlouho se používá nový NTor protokol

Sibyl attack

- spuštění mnoho instancí Tor relayů jedním útočníkem, typicky na jednom stroji
- je to relativně jednoduše zjistitelné
- v Tor project je dobrovolník, který takové věci sleduje

DNS leak

- u běžných protokolů předchází IP spojení vyhledání v DNS
- u Toru se toto musí potlačit
  - Tor Browser Bundle to umí
- ostatní nástroje a programy leakují rády, protože na tohle nejsou stavěny
  - torsocks utilita může pomoci
- root DNS servy vidí taky mnoho „netrefených“ .onion DNS dotazů

Útok na aplikaci mimo Tor

- neútočíte na Tor, útočíte na PC, kde běží
- z hlediska útočníka nejjednoduší
- největší „attack surface“
- na klienta: exploit browseru
  - věci jako Flash zásadně nepoužívat
  - operace Torpedo
- na hidden service: exploit serveru
  - takhle chytili Ulbrichta ze Silk Road

RELAY/RELAY EARLY

- kombinace mnoha předchozích útoků
- jeden z technicky nejlepších útoků na Tor
- FBI si ho objednala od Carnegie Mellon University za řádově $1M
  - FBI dlouho o tom mlžila
- deanonymizace IP klienta a hidden service
- jeho výsledky hráli roli v uzavření mnoha HS v Operation Onymous

RELAY/RELAY EARLY (2)

- pravděpodobností útok (!!!)
  - umí deanonymizovat „jen“ pár endpointů
- útočník musí ovládat Guard node klienta nebo HS, který je v circuitu
- a zároveň ovládat HSDir node, kde se bude klient ptát
- normálně se circuit rozšiřuje přes RELAY cell

RELAY/RELAY EARLY (3)

- zákeřné nody způsobí rozšíření „circuitu“ kombinací RELAY a RELAY EARLY „cells“
  - kde RELAY značí 0 a RELAY EARLY 1
- zakódují tak název hidden servicu
- je zapotřebí ovládat velké množství nodů
  - plus další podmínky jako velká rychlost
- v praxi se to skombinovalo se „sibyl attack“

Děkuji za pozornost

hiviah • hiviah@torproject.org