What *does* TOR do?

• TOR is just an additional layer of obscurity. No more, no less.

• Provides unlisted, bridge relays to solve problems in reaching the first relay
  • e.g. ISP filtering connections to any known TOR relays
  • Bridges can’t be easily identified, so can’t be blocked

• Without TOR, everything one does online can be watched by one’s ISP
  • Anything passing through a tapped internet exchange point can be stored and analyzed by intelligence agencies
What doesn’t TOR do?

• Anonymize users; it only anonymizes that computer
  • No security if a user provides personal information to another service
  • VPN’s with logs subject to subpoena also a concern

• Provide protection against end-to-end timing attacks
  • Watching the traffic at both ends of communication can result in a compromised link

• Allow users to indulge in unsafe behavior
  • Maybe don’t use your legal name? More on this...
How Safe is TOR?

• Strong crypto systems are one of the few things you can rely on

• Version 2.3.25-13 most common
  • Uses 1024 RSA/Diffie-Hellman crypto

• Version 2.4.17-beta-2 also available
  • Uses Elliptical Curve Diffie-Hellman (ECDH)
  • Can yield same level of security with 164 bits as RSA/DH can with 1024 bits
How Safe is TOR?

• Tor 2.4 based on the elliptic curve discrete logarithm problem
  • Finding the discrete logarithm of a random elliptic curve element with respect to a publicly known base point
  • Currently assumed to be infeasible

• Very easy to do, very hard to reverse
  • Perfect for crypto
What are the risks?

• Vast majority (~90%) of TOR users still use version 2.3, and its 1024 bit DH crypto
  • NSA can break this in a few hours using brute force attacks
    • Not in real-time, only possible on targeted, archived offline data
    • Needs custom-built chips
  • Has publicly known contracts with IBM

• Version 2.4 and ECDH might still be within NSA’s, and others’, scope
  • Less popular, so likely less money/time/effort put into breaking ECDH

• A hidden service website that made mistakes in configuration or maintenance could compromise anonymity independent of TOR
ESIEA “broke” TOR?

• École Supérieure d’Informatique, Électronique, Automatique
  • French ‘Grande École’ for private engineers

• Performed inventory of the TOR network and developed a script to identify the TOR Bridges
  • Found 6,000 relays and 181 Bridges
  • Claimed to have a “complete picture of the topography of TOR”

• Research claims that one third of TOR nodes are vulnerable
ESIEA “broke” TOR?

- Engineered a virus in a lab setting aimed at infecting and obtaining system privileges of TOR nodes
  - Infected nodes are cloned to create a local network in the lab

- Traffic is directed to infected nodes by a double attack on the network
  - Denial of Service attack on clean nodes
  - Packet spinning, creating a loop within TOR servers to lead the packet to an infected node

- An infected node as a second relay would be a big problem
How the Silk Road was shut down

• Evolution of law-enforcement problems:
  • Dread Pirate Roberts vs. Al Capone
  • Problem with identification, not incrimination
  • Silk Road only accessible through TOR, only used BitCoins

• Two year long investigation led by Christopher Tarbell and “Agent-1”
  • Agent-1 ironically anonymous
  • Theories that Agent-1 is Hector Xavier Monsegur, also known as Sabu
  • Sabu was a leader of the group Anonymous, and was arrest by Tarbell in June 2011
How the Silk Road was shut down

• January 27, 2011
  • Username *altoid* found on a discussion forum discussing psychedelic mushrooms
  • *altoid* found again on a BitCoin discussion forum on January 29

• Eight months later
  • *altoid* posts to a BitCoin forum again, looking to hire an IT pro
  • Includes contact information (personal email address) : Ross Ubricht

• Dread Pirate Roberts and Ubricht had strongly overlapping online activity (same videos, links, timezone, etc…)
  • Silk Road was run through a private, unique access VPN
  • Tarbell and Agent-1 traced it to an IP-address
  • Traced IP and Ubricht’s Comacst IP were within 500 feet
Points to Ponder

- Silk Road bust had nothing to do with breaking TOR. Most successful raids have been through subpoenaed banks, VPN’s, etc…

- ESIEA’s attempt to break TOR is still in its infancy; it has too small a reach on the Internet given the sheer number of TOR relays. But if French, British and American intelligence traded their data, could TOR be broken?

- If TOR is broken, would we find out? If so, how quickly?
Sources

• TOR’s weakness to brute-force attacks
  • “Majority of Tor crypto keys could be broken by NSA, researcher says”, by Dan Goodlin

  • “90 percent of Tor keys can be broken by NSA: what does it mean?”, by Cory Doctorow
    http://boingboing.net/2013/09/07/90-percent-of-tor-keys-can-be.html

  • “NSA works with security vendors to thwart encryption, according to 'Bullrun' docs leaked by Snowden”, by Xeni Jardin
    • http://boingboing.net/2013/09/05/report-nsa-slices-through-mos.html
Sources

• Elliptical Curves in TOR 2.4
  • “Elliptical curve cryptography (ECC)”, by Margaret Rouse
    http://searchsecurity.techtarget.com/definition/elliptical-curve-cryptography

• ESIEA’s Map of TOR
  • “Tor anonymizing network Compromised by French researchers”, by Mohit Kumar