Covert Channels

from Merike Kaeo

merike@doubleshotsecurity.com

Modified by Cristel Pelsser

Covert Channels

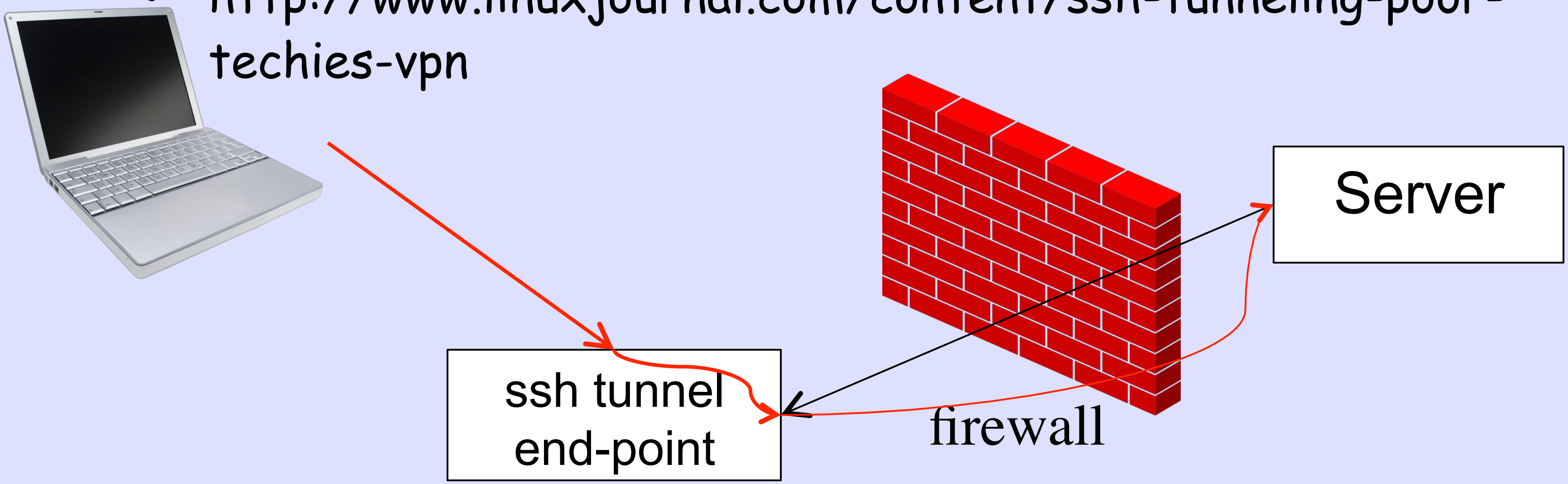
- Tunnels that are used to bypass filters and intrusion detection systems
  - Use traffic that is thought to be something else (i.e. DNS tunnels)
  - Can also provide encryption (i.e. SSH tunnels)
- Some instances of use:
  - Hotels that block specific ports
  - Countries that block some access
- Other mechanisms use obfuscated paths with encryption (TOR)

DNS Tunneling

- Uses DNS to hide your traffic
- Can also be used maliciously to sneak public hotspots which are protected by HTTP redirections only
    - Those hotspots will allow web traffic to some few restricted websites (or some login page) only, but often allow all DNS traffic
- How: embed an IP packet inside what looks like a DNS query
- HowTo references
    - http://dnstunnel.de/
    - http://code.kryo.se/iodine/

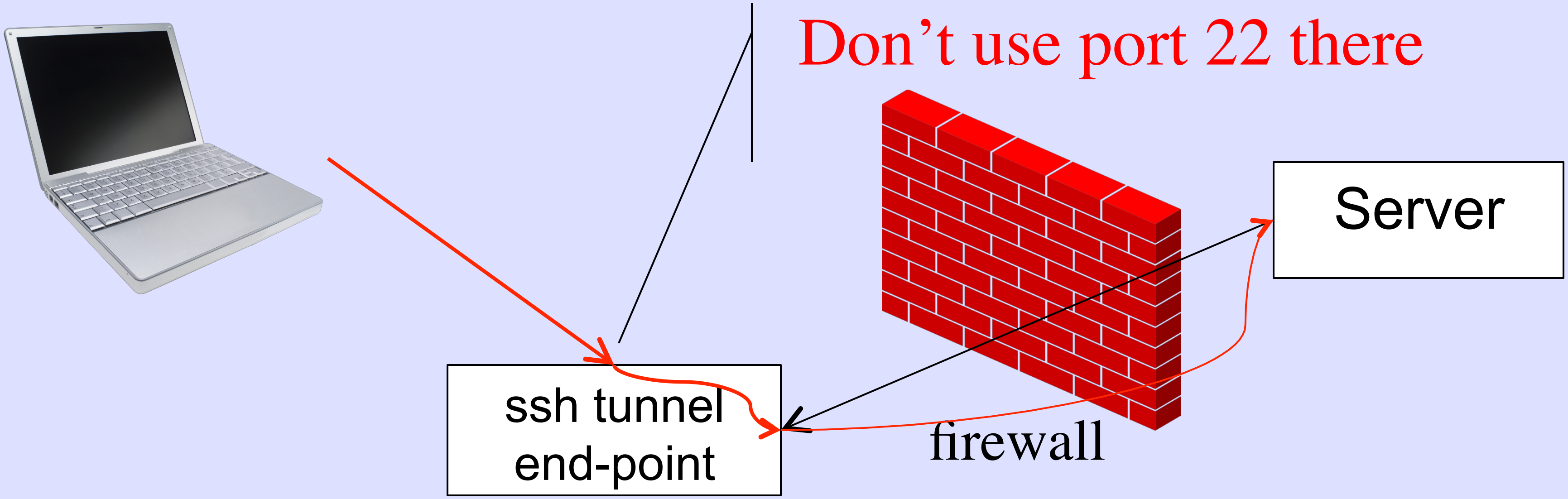
SSH Tunneling

- Traffic is tunneled thru SSH
- Reverse tunneling lets you create a tunnel from a server that is behind a firewall with no SSH servers to an SSH server.
- HowTo for SSH Tunneling
  - http://www.linuxjournal.com/content/ssh-tunneling-poor-techies-vpn



SSH Tunneling

- Brute force attacks more common these days
  - Don't use 22 as external port on the relay
  - Open source software available to prevent brute force attacks on OpenSSH while also providing Two-Factor Authentication for OpenVPN and Web Single Sign On.
  - http://taferno.sourceforge.net



TOR -Onion Routing

- Originally a project from the US Naval Research Laboratory
- Prevents traffic analysis
  - Recall that military intelligence agencies rely heavily on traffic analysis
- Developed for the U.S. Navy in mind, primarily to protect government communications
- Today, it is used every day for a wide variety of purposes by normal people, the military, journalists, law enforcement officers, activists, and many others.

TOR – What Is It?

- Allows **anonymity** in the Internet
- Prevents anyone from learning your location or browsing habits
- Open source and available for many varying OSs
  - Windows, MAC, LINUX/UNIX, Android
- Also allows for users to **hide their locations** while offering various kinds of services

Why TOR

- Traffic analysis can be used to infer who is talking to whom over a public network
- Knowing the source and destination of your Internet traffic allows others to track your behavior and interests
- E-commerce site uses price discrimination based on your country or institution of origin
- Even if you encrypt the data payload, traffic analysis still reveals a great deal about what you're doing and, possibly, what you're saying.
    - That's because it focuses on the header, which discloses source, destination, size, timing, etc.

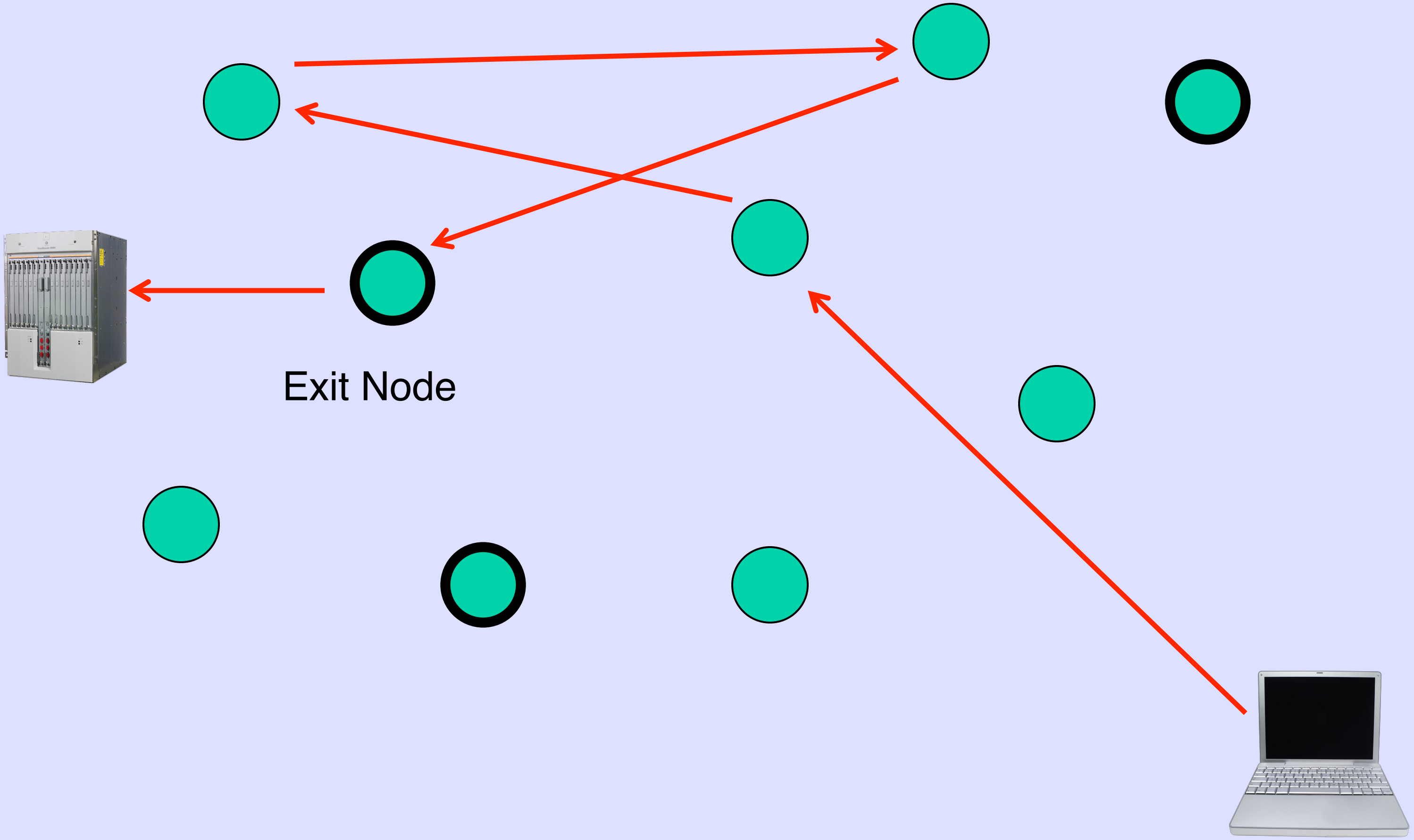
Setting The Path

- The user's TOR client obtains a list of TOR Nodes from a directory server and incrementally builds a circuit of encrypted connections through TOR relays on the network
- The circuit is extended one hop at a time
    - Each relay along the way knows only which relay gave it data and which relay it is giving data to
- No individual relay ever knows the complete path that a data packet has taken
- The client negotiates a separate set of encryption keys for each hop along the circuit

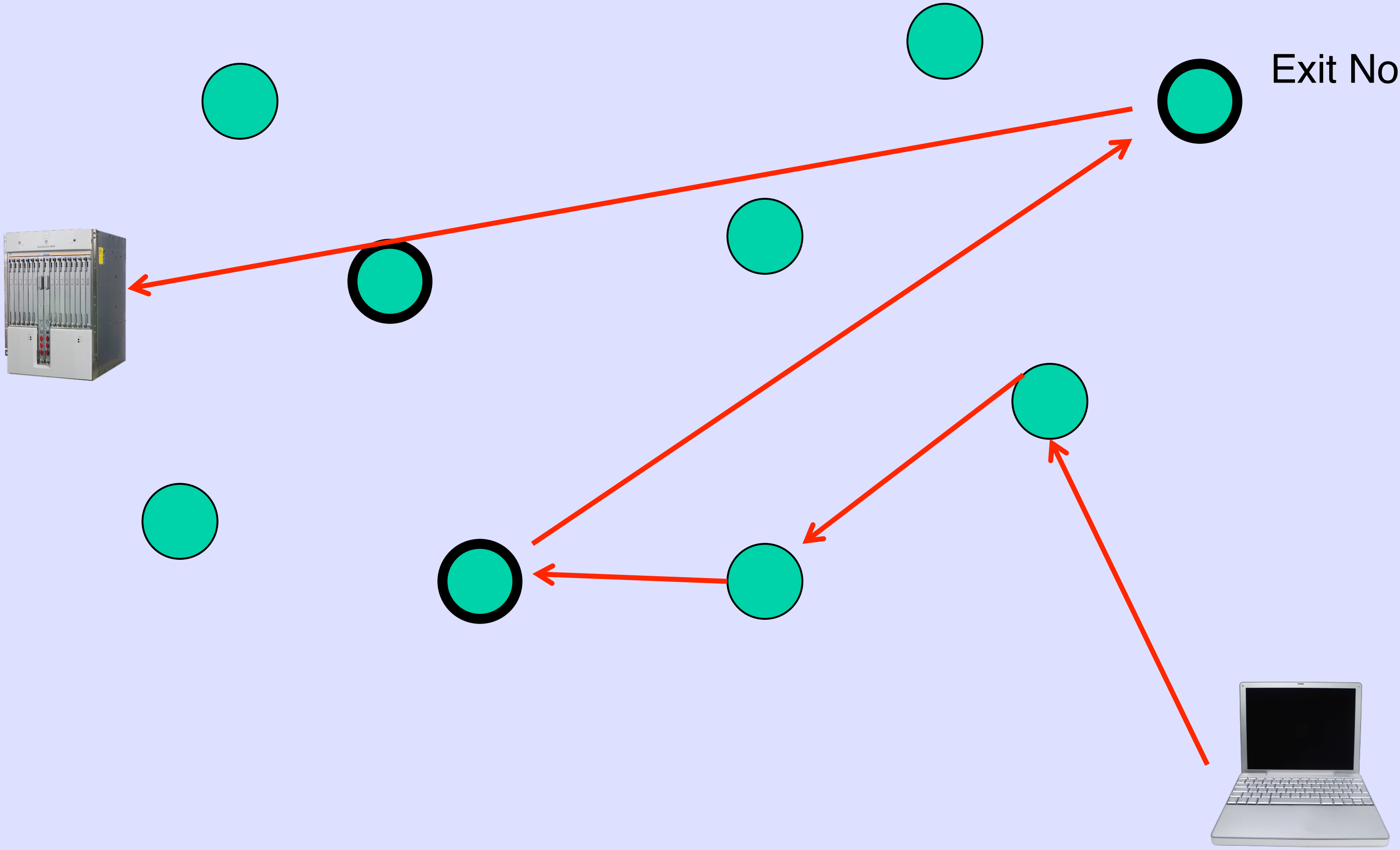
How TOR Works

- Neither an eavesdropper nor a compromised relay can use traffic analysis to link the connection's source and destination
  - Each relay sees no more than one hop in the circuit
  - Adversary can watch some links and nodes, but not all
- TOR only works for TCP streams and can be used by any application with SOCKS support
- TOR software uses the same circuit for connections that happen within the same ten minutes or so
- Later requests are given a new circuit, to keep people from linking your earlier actions to the new ones

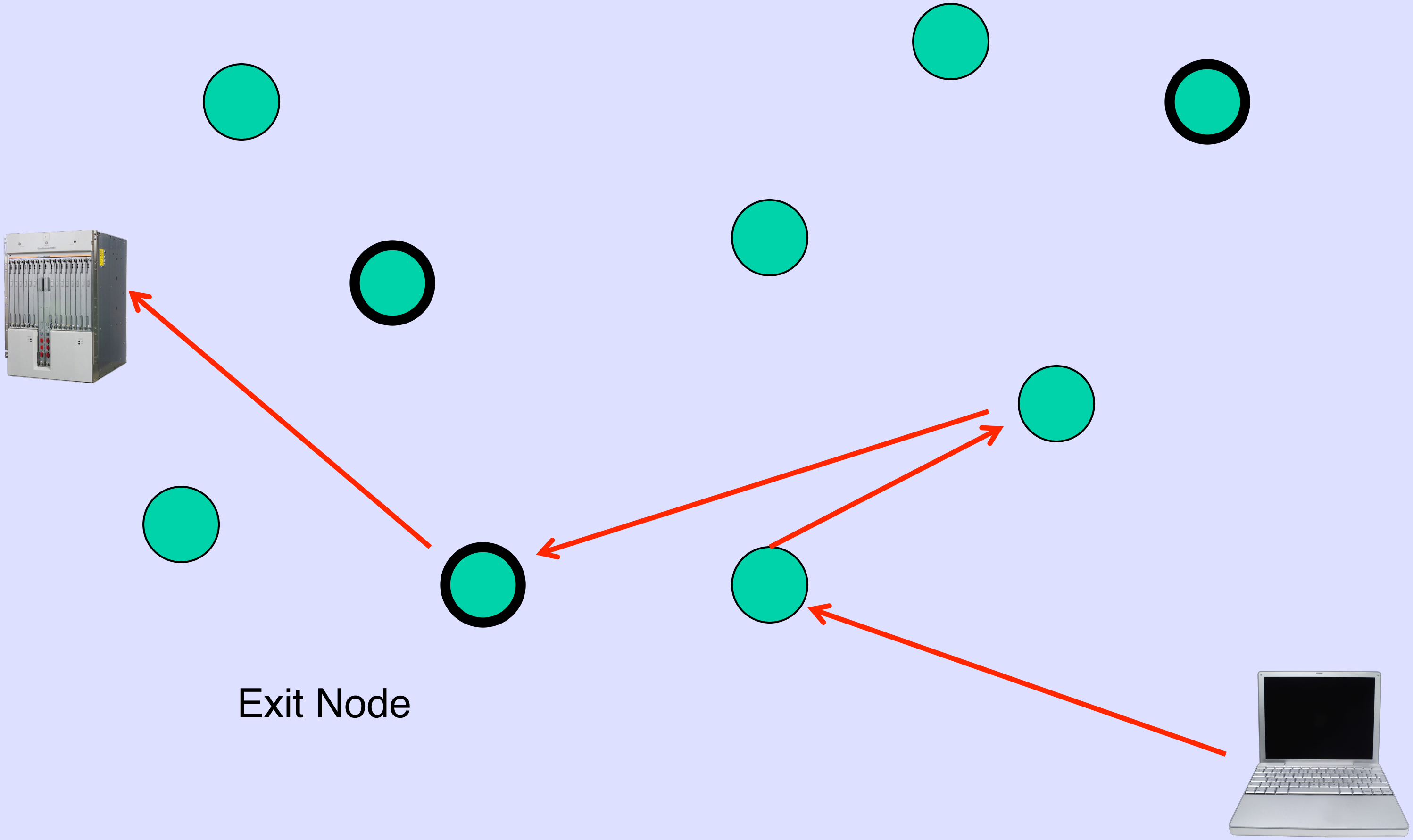
How Tor Works: One Visit



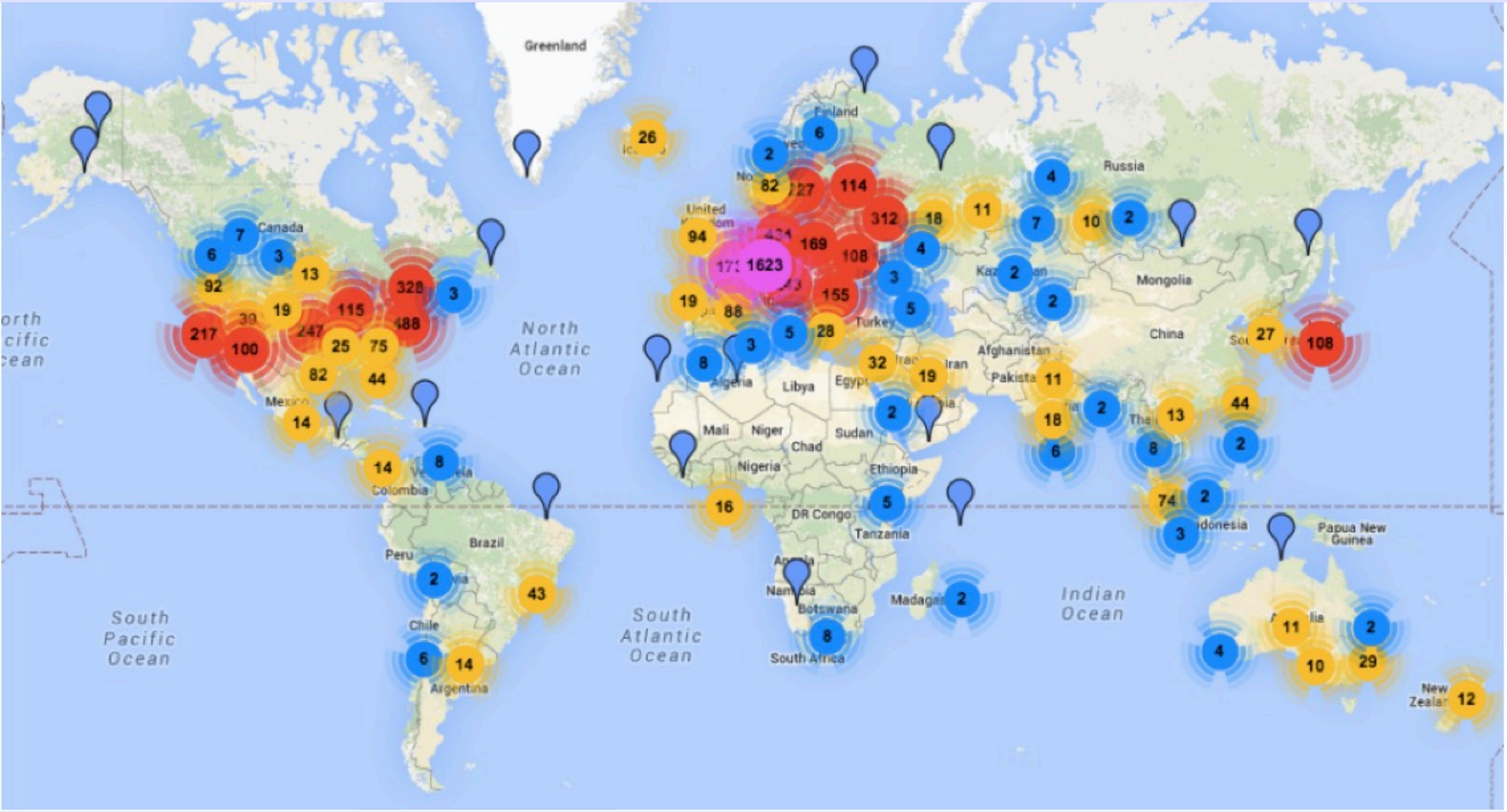
How Tor Works: Another Visit



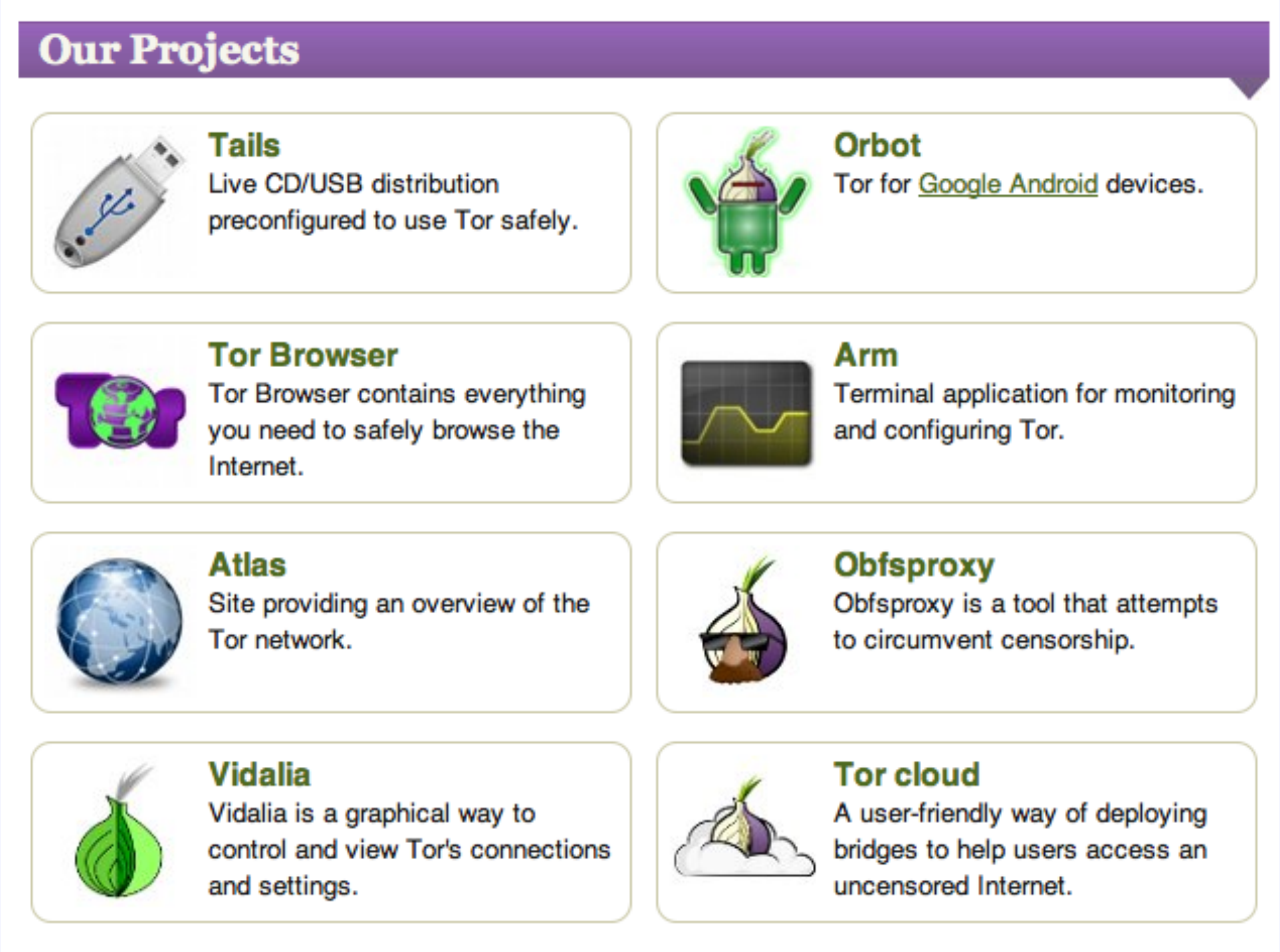
How Tor Works: Another Visit



Distributed Relays



https://www.torproject.org/



Our Projects

Tails
Live CD/USB distribution preconfigured to use Tor safely.

Orbot
Tor for Google Android devices.

Tor Browser
Tor Browser contains everything you need to safely browse the Internet.

Arm
Terminal application for monitoring and configuring Tor.

Atlas
Site providing an overview of the Tor network.

Obfsproxy
Obfsproxy is a tool that attempts to circumvent censorship.

Vidalia
Vidalia is a graphical way to control and view Tor's connections and settings.

Tor cloud
A user-friendly way of deploying bridges to help users access an uncensored Internet.

Steganography

- Derived from the Greek *steganos*, meaning covered or secret, and *graphy*, meaning writing or drawing
- Literally means covered writing
- The practice of concealing a message to casual observers—the content is there in the open, and often unencrypted
- In its most common modern digital form, steganography conceals plain text or whole files within an image, audio, or video file

Simple Example

- Take an uncompressed image: a 2048×1024×3 array of bytes
- Put your message in the low-order bits of certain bytes
  - Changing low-order bits creates an imperceptible change in color for those pixels
- For greater security, encrypt the message first: encrypted data looks like uniformly distributed random bits
  - Use a PRNG to select which bytes contain your bits
- Many tools listed at
- http://en.wikipedia.org/wiki/Steganography_tools

Detecting Steganography Data

- Stegananalysis is difficult (stating the obvious)

- The use of application "fingerprint" data—artifacts and patterns in files that show they've been manipulated by steganography tools

- Some companies have a steganography fingerprint database that contain identifying information for known digital steganography applications

- Databases are integrated into real-time scanners that sit at the edge of a network