Covert Channels

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)

Covert Channel

- If you feel the need to use DNS, SSH or any other tunneling technique to bypass your corporate firewall make sure you are not violating any of your company's Internet Acceptable Use Policy

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/

DNS Tunneling Tools

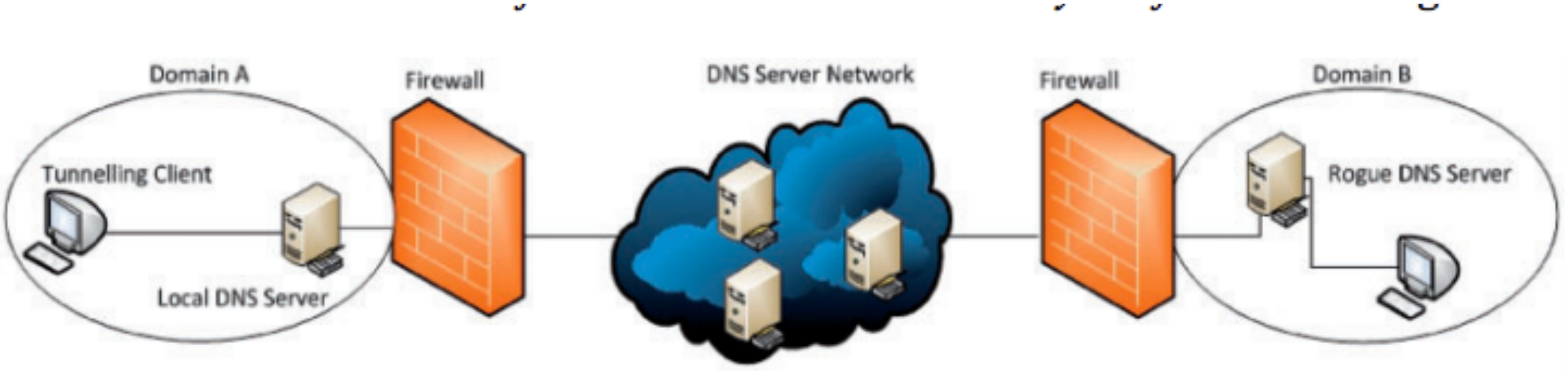


FIG. 1. Entities involved in a DNS Tunnel.

* DNS2TCP
Dns2tcp is a network tool designed to relay TCP connections through DNS traffic. Encapsulation is done on the TCP level, thus no specific driver is needed (i.e: TUN/TAP). Dns2tcp client doesn't need to be run with specific privileges.

* TCP-OVER-DNS
tcp-over-dns contains a special dns server and a special dns client. The client and server work in tandem to provide a TCP (and UDP!) tunnel through the standard DNS protocol.

SSH Tunneling

- Traffic is tunneled thru SSH
- "Poor-techie's VPN"
- One configures an SSH client to forward a specified local port to a port on the remote machine
- HowTo for SSH Tunneling
  - http://www.linuxjournal.com/content/ssh-tunneling-poor-techies-vpn

SSH Tunnel

- Typical SSH tunnel
  - ssh -N -p 22 user@mylinuxserver.net -L 2110:localhost:110
- Forward google talk
  - ssh -g -p 2022 -N bob@mylinuxserver.xxx 5223:talk.google.com:5223
- Forward which protocols?
  - ssh -N -p 2022 bob@mylinuxserver.xxx -L 2110:localhost:110 -L 2025:localhost:25

TOR – The Onion Routing

- Originally a project from the US Naval Research Laboratory
- Developed for the U.S. Navy in mind, primarily to protect government communications
- Prevents traffic analysis
  - Recall that military intelligence agencies rely heavily on traffic analysis
- 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.

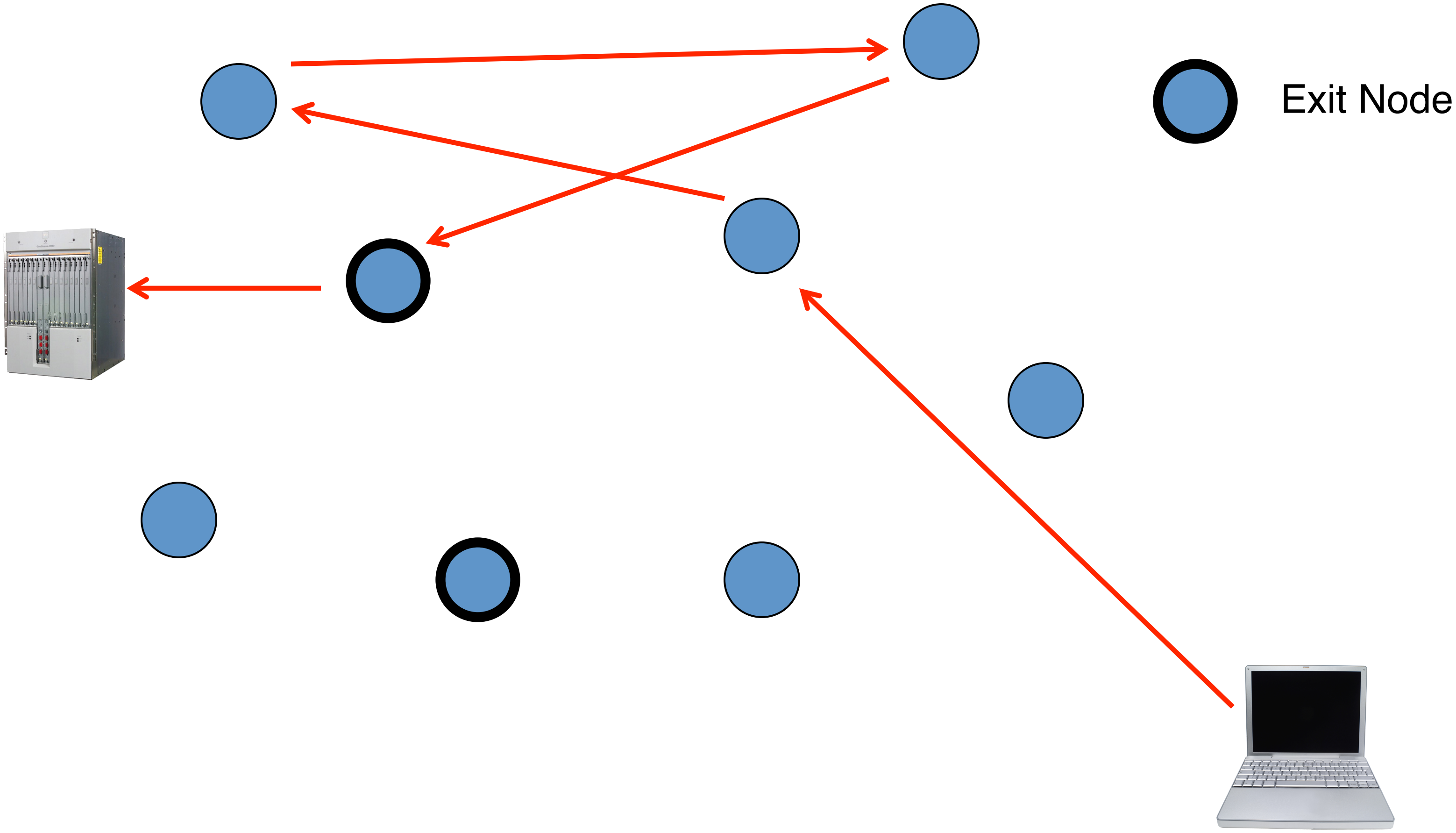
How TOR Works – Setting The Path

- 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

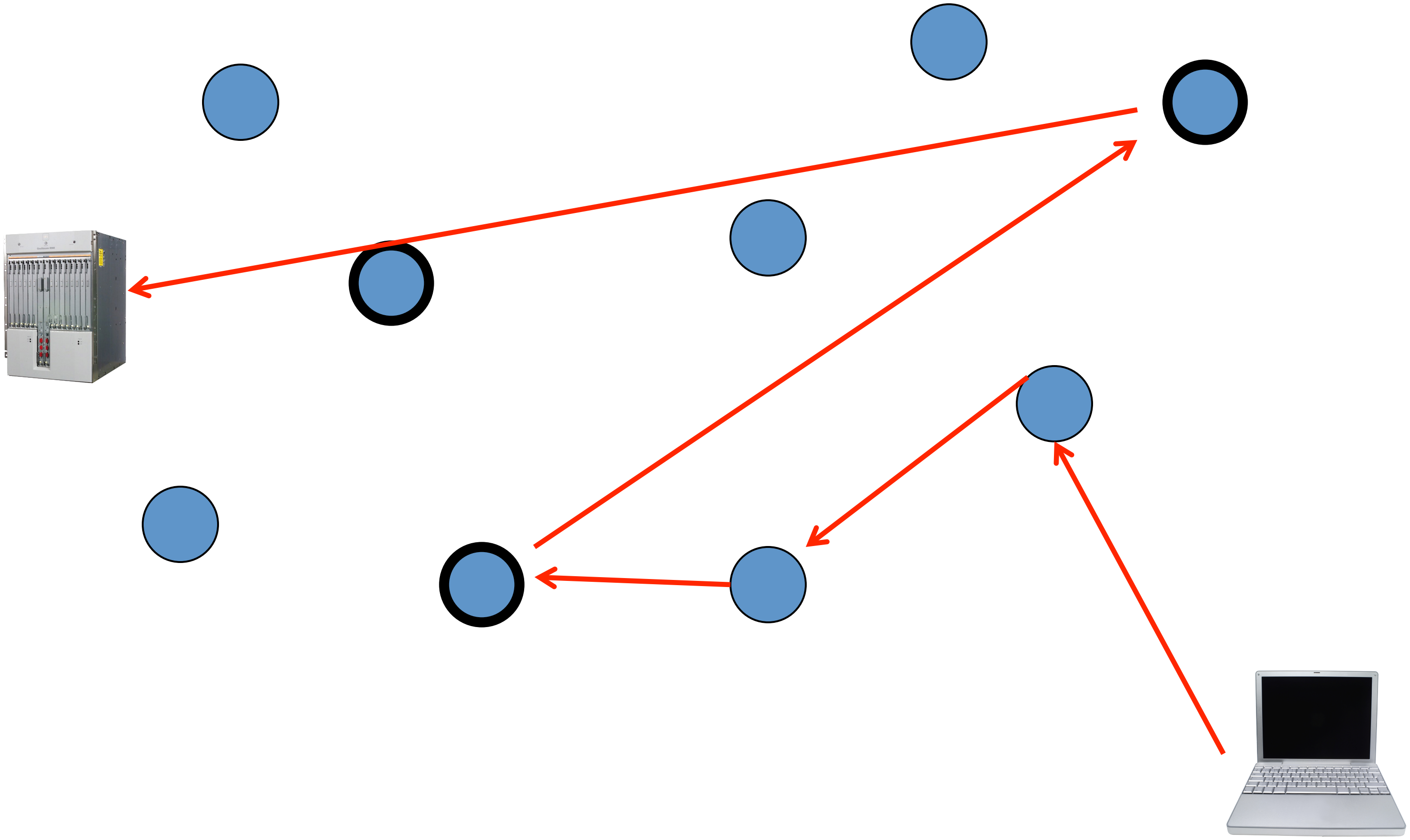
- Neither an eavesdropper nor a compromised relay can use traffic analysis to link the connection's source and destination
  - Each relay sees no more than one hop in the circuit
  - Adversary can watch some links and nodes, but not all
- TOR only works for TCP streams and can be used by any application 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: First Visit

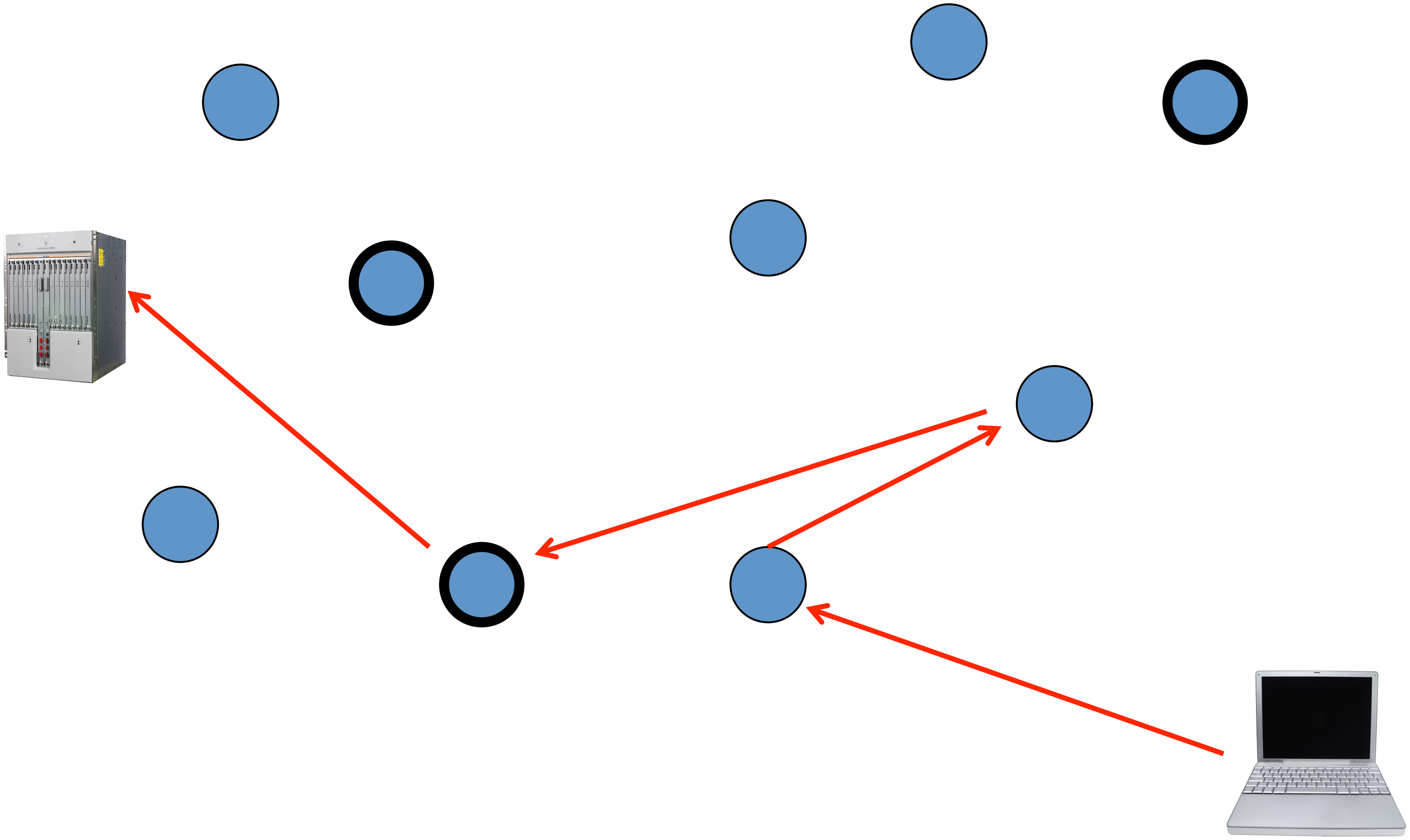


Exit Node

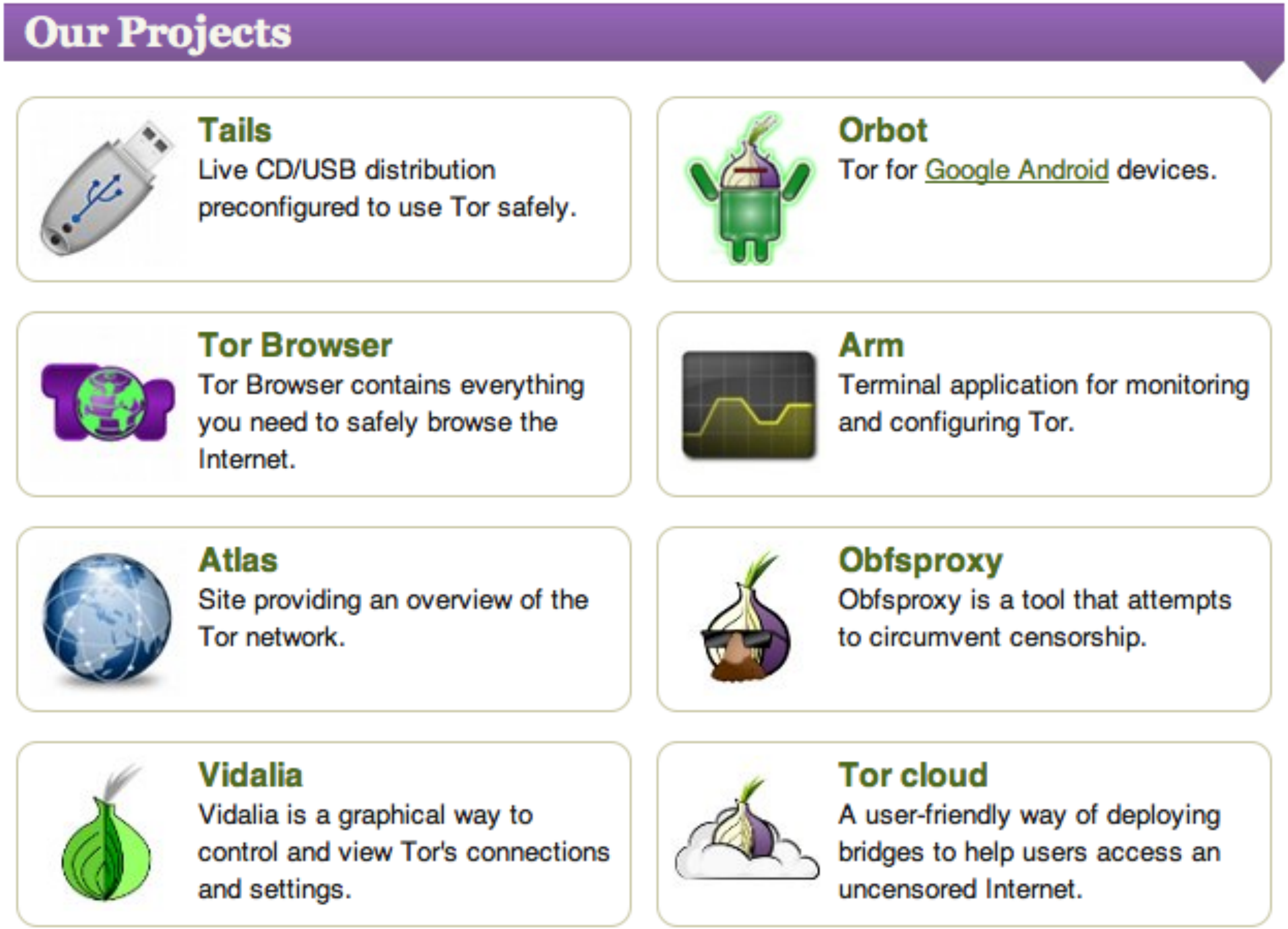
How Tor Works: Second Visit



How Tor Works: Third Visit



More on TOR: 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
  - invisible inks, tiny pin punctures on selected characters, minute differences between handwritten characters, pencil marks on typewritten characters, hiding messages in graphic images
- In its most common modern digital form, steganography conceals plain text or whole files within an image, audio, or video file

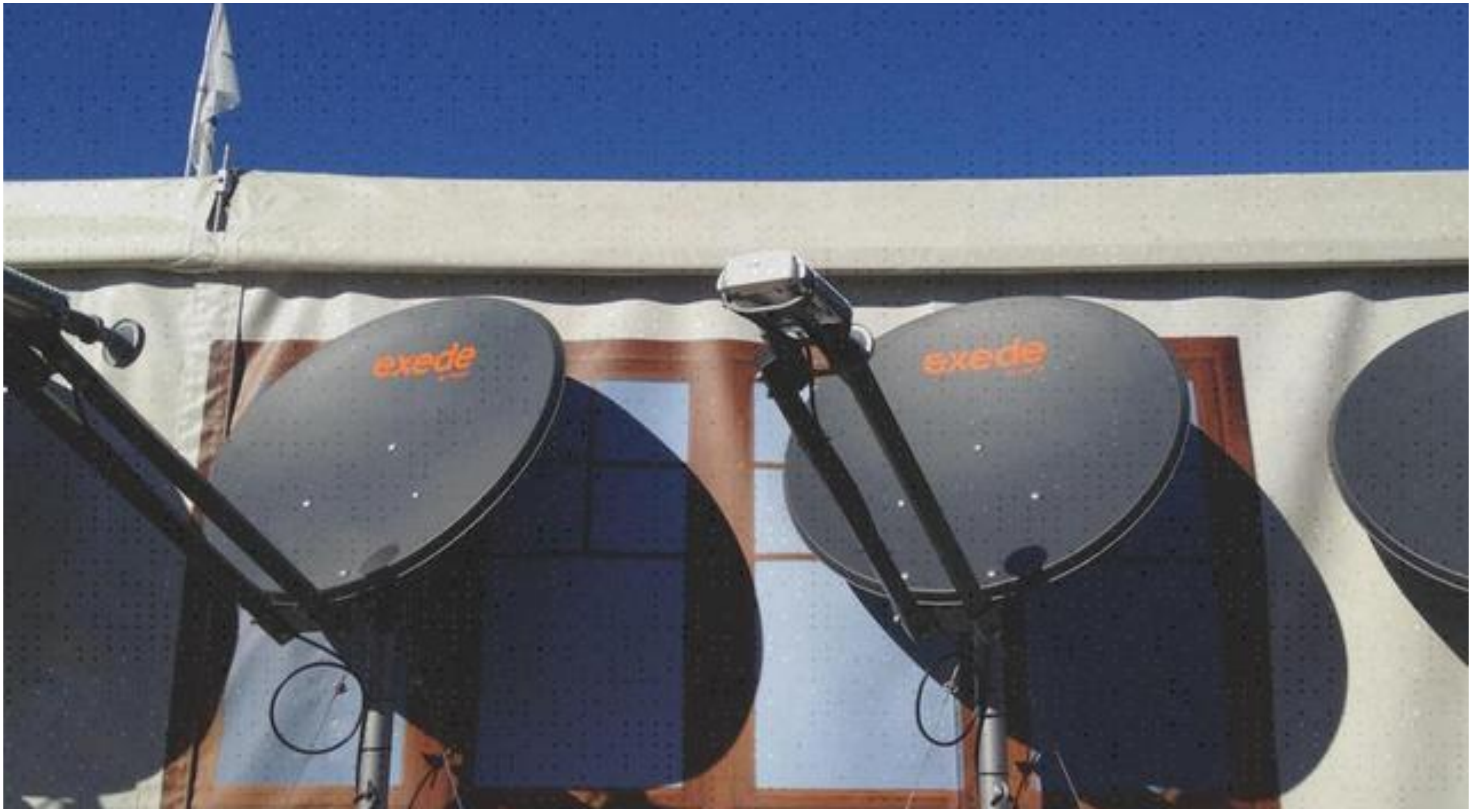
Steganography Examples

- Invisible Ink
  - Open a JPEG file in a text editor, append the text at the end of the content
  - Mostly used with software tools to become more subtle
    - http://diit.sourceforge.net/background.html
- Hiding the cosine
  - Using RGB colorspace
- More sophisticated tools

Steganography: 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

Invisible Ink Example



Invisible Ink Example

Example – Al Qaeda Hid Documents in a Porn Video

- Al-Qaeda member arrested in Berlin in 2011
- He has a memory card with password-protected folder with hidden files
- German Federal crime police uncovered a pornographic video
  - 141 separate text files within the video
  - Contains operations and plans for future operation

http://arstechnica.com/business/2012/05/steganography-how-al-qaeda-hid-secret-documents-in-a-porn-video/

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