CIPHERSPACES/DARKNETS: AN OVERVIEW OF ATTACK STRATEGIES

Adrian Crenshaw

tenacity solutions

About Adrian

- I run Irongeek.com
- I have an interest in InfoSec education
- I don't know everything - I'm just a geek with time on my hands
- (ir)Regular on the ISDPodcast http://www.isdpodcast.com
- Researcher for Tenacity Institute http://www.tenacitysolutions.com

A little background…

- Darknets: There are many definitions, but the one I'm working from is "anonymizing networks"
- Use of encryption and proxies (some times other peers) to obfuscate who is communicating to whom
- Sometimes referred to as Cipherspace (love that term)
- Tor and I2P will be my reference examples, but there are others

…and some notes

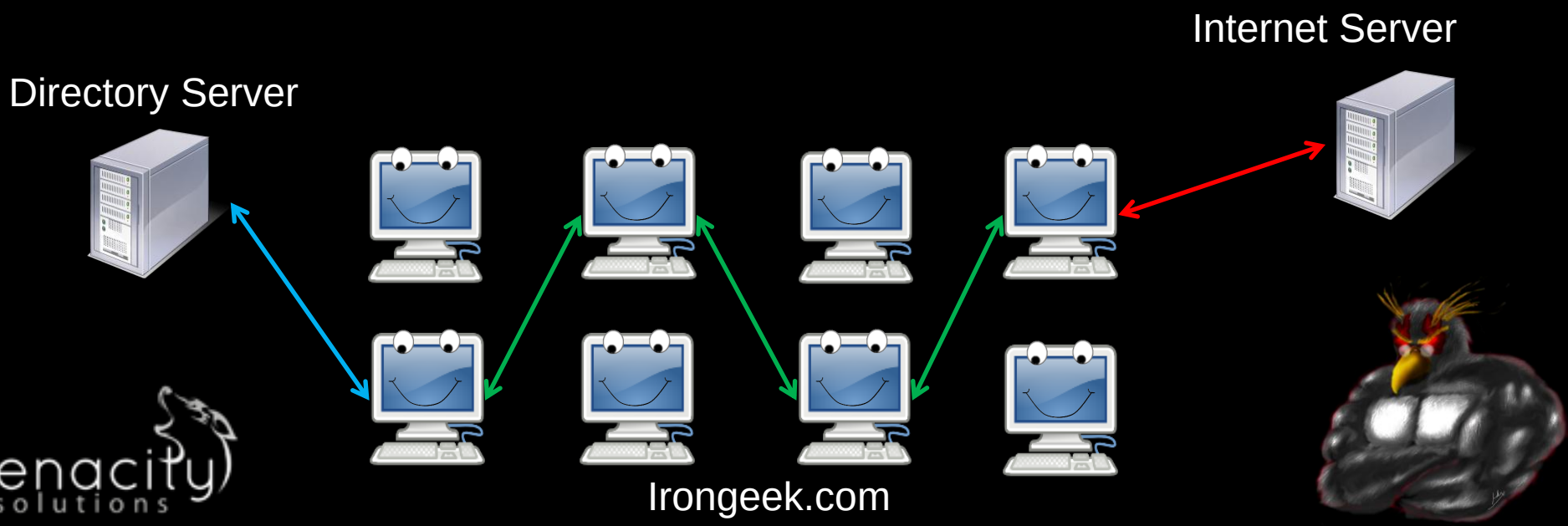
- Things get subtle
- Terms vary from researcher to researcher
- Many weaknesses are interrelated
- Other anonymizing networks: Morphmix/Tarzan/Mixminion/Mixmaster/JAP/MUTE/AntsP2P/Haystack
- Focus on Tor and I2P for illustrations when needed
- Academic vs. real world

Threat Model and Adversaries matter

- Threat Model: You can't protect against everything!
  - Some protocols may be lost causes
  - Users may do something to reveal themselves
  - Does an attack reveal the Client/Host or just reduces the anonymity set?
- Active vs. Passive attackers
- Location, Location, Location:
  - Internal vs. External
- Adversaries: Vary by power and interest
  - Nation States
    - Western Democracies vs. Others
  - Government agency with limited resources
  - ISP/Someone with a lot of nodes on the network
  - Private interests groups (RIAA/MPAA)
  - Adrian (AKA: Some shmuck with time on his hands)

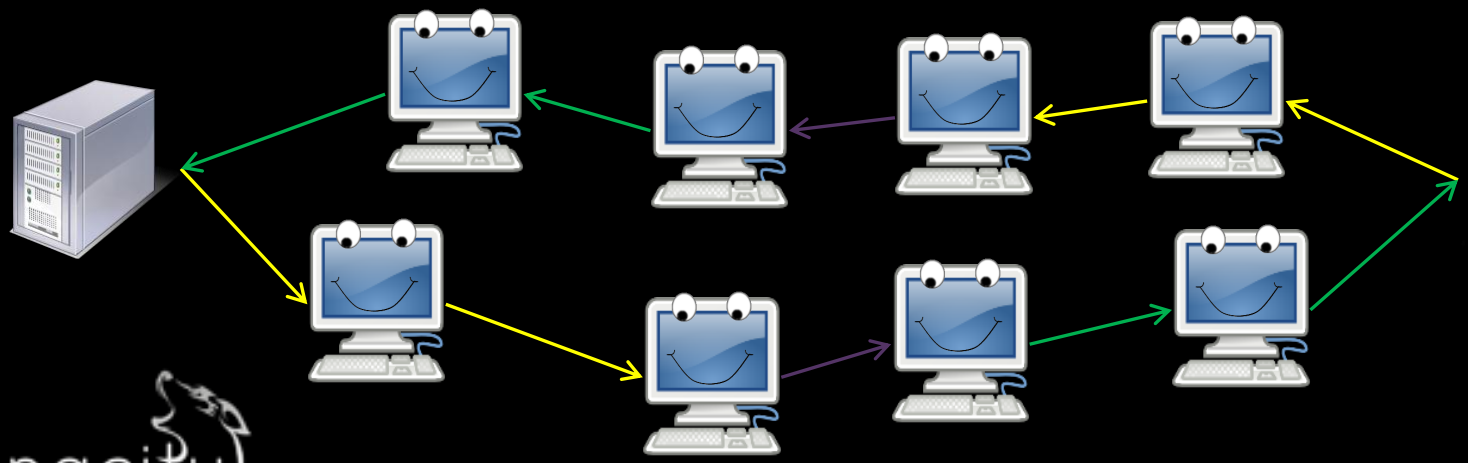
Tor: The Onion Router

- Layered encryption
- Bi-directional tunnels
- Has directory servers
- Mostly focused on out proxying to the Internet
- More info at https://www.torproject.org



I2P

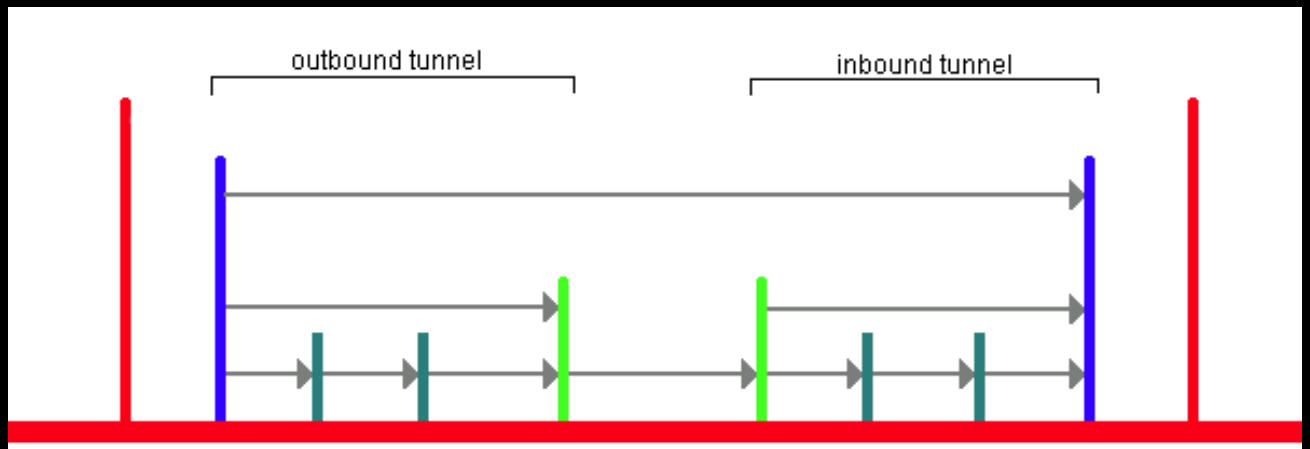
- Unidirectional connections: In tunnels and out tunnels
- Information about network distributed via distributed hash table (netDB)
- Layered encryption
- Mostly focused on anonymous services
- More info at http://www.i2p2.de/



tenacity solutions

I2P Encryption Layers

- EIGamal/SessionTag+AES from A to H
- Private Key AES from A to D and E to H
- Diffie–Hellman/Station-To-Station protocol + AES



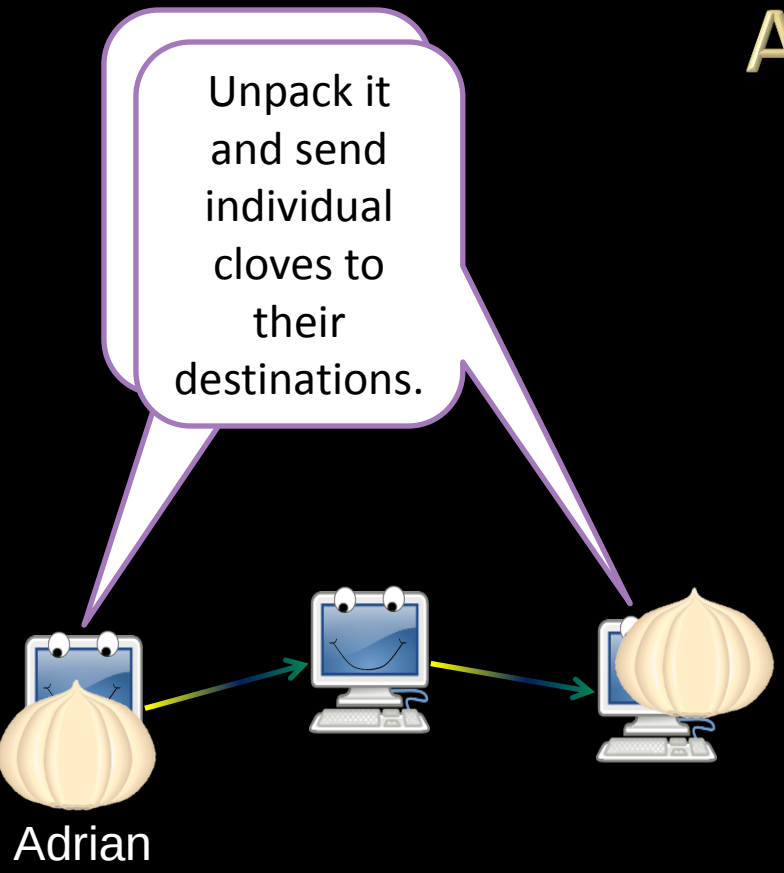
		tunnel encryption (private key AES)	a to d, e to h
garlic encryption (ElGamal/SessionTag+AES)	a to h	transport encryption (DH/STS+AES, etc)	a to b, b to c, c to d, d to e, e to f, f to g, g to h

Image from http://www.i2p2.de/

Irongeek.com

tenacity solutions

Silly Garlic Routing Animation



tenacity solutions

Irongeek.com

UN-TRUSTED EXIT POINTS

You are only as anonymous as the data you send!

Overview

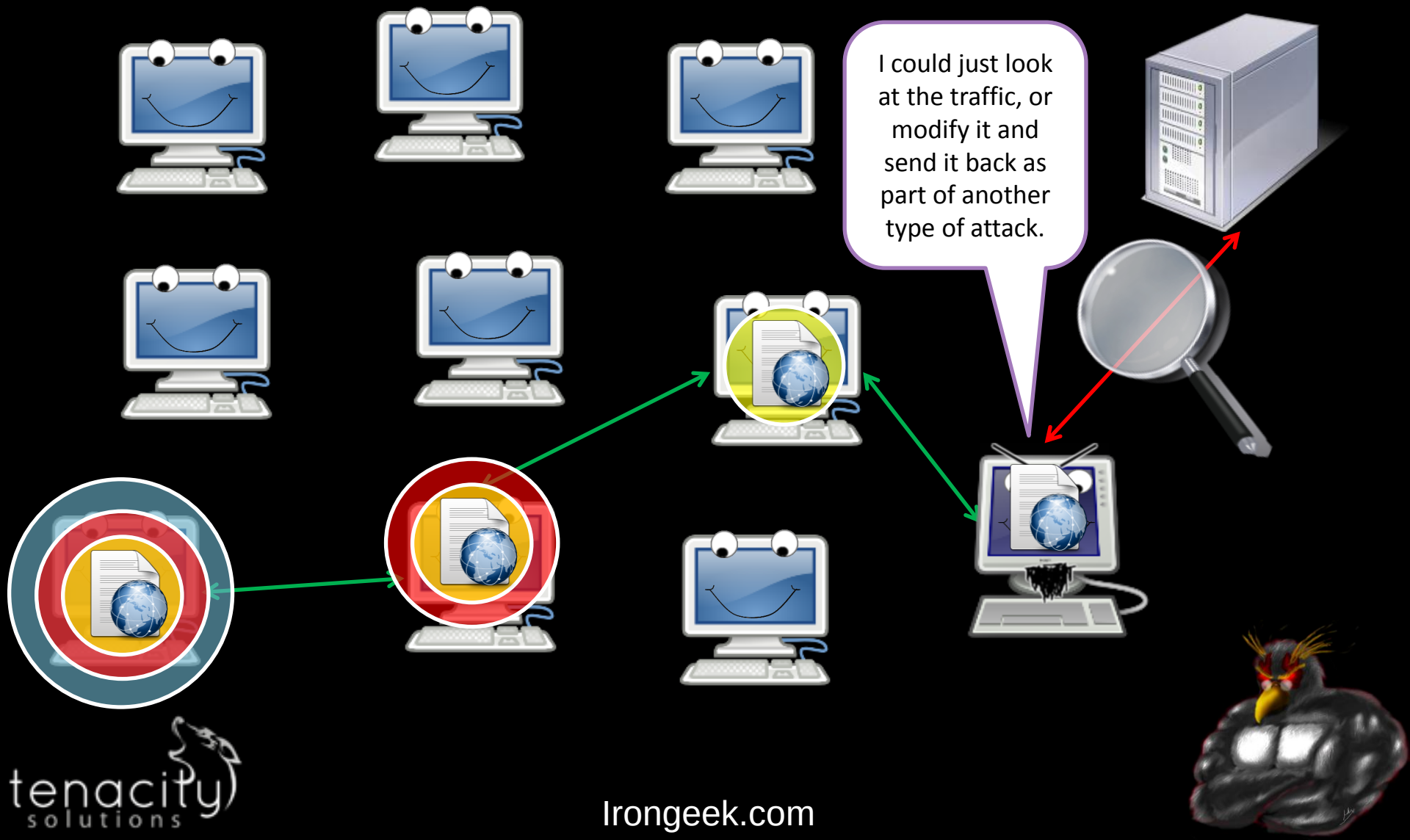
Mostly Tor centric:

- Is the exit point for traffic looking at the data?
- Traffic may be encrypted inside the network, but not once it is outbound!

Incidents

- Dan Egerstad and the “Embassy Hack” http://www.wired.com/politics/security/news/2007/09/embassy_hacks
- Tons of passwords sent via plain text protocols (POP3/SMTP/HTTP Basic/Etc)
- Moxie Marlinspike did something similar with SSLStrip http://intrepidusgroup.com/insight/2009/02/moxie-marlinspike-un-masks-tor-users/

Do you trust your exit node?



tenacity solutions

Irongeek.com

Mitigation

- Tor is for anonymity, not necessarily security
- Use end-to-end encryption/Don't use plain-text protocols
- Plain text protocols that send usernames/email addresses in the clear are not very anonymous now are they?

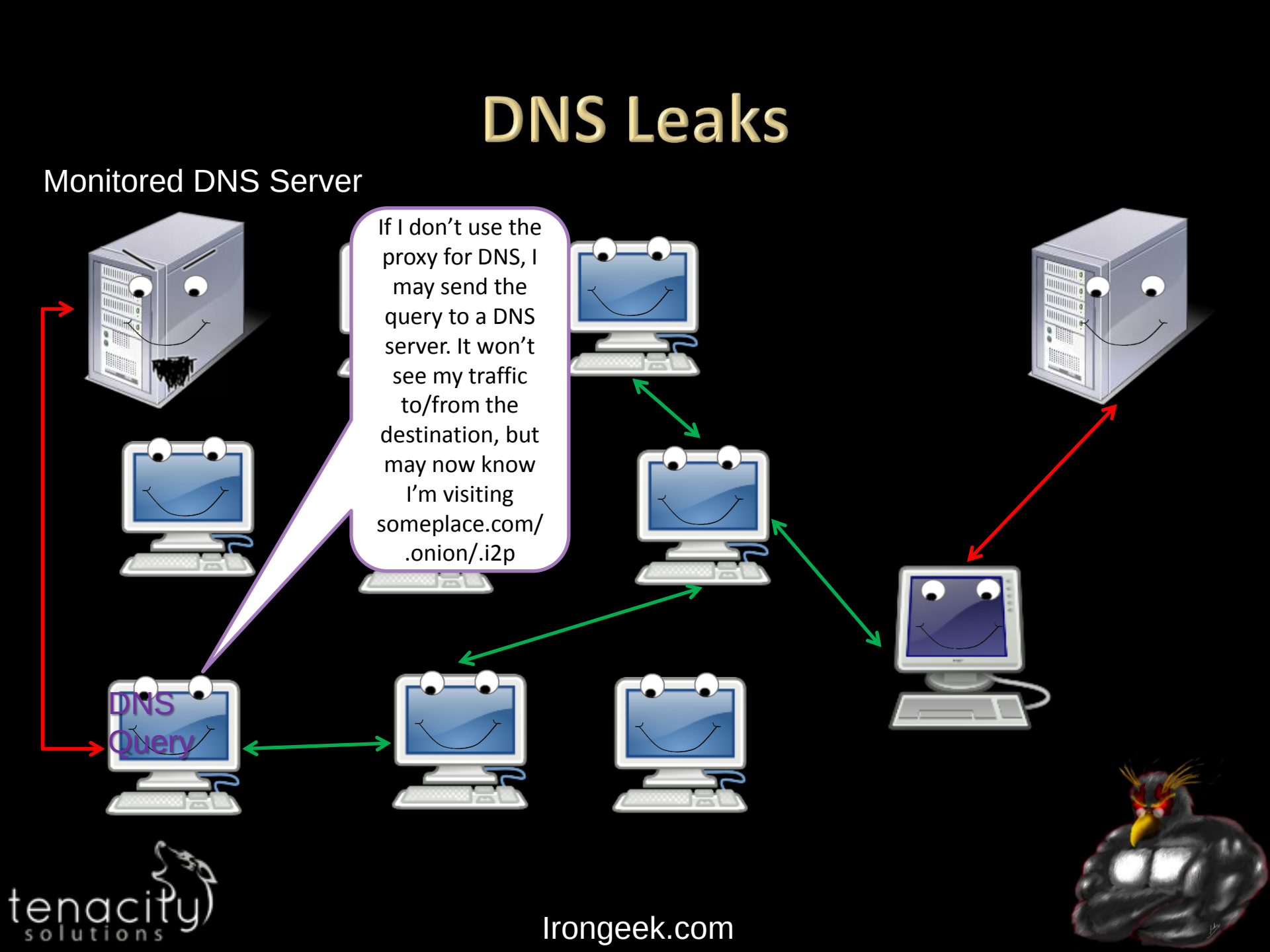
DNS LEAKS, OTHER PROTOCOL LEAKS AND APPLICATION LAYER PROBLEMS

tenacity solutions

Overview

- Does all traffic go though the proxy?
- DNS Leaks are a classic example
- Badly configured proxy setting could lead some types of traffic to go elsewhere (outside of cipherspace)
- Snooper can use web bugs to figure out your location
  http://www.irongeek.com/i.php?page=security/webbugs
- HTTPS is a good example, but plugins can also be an issue
- Application level stuff in general is a problem
- Javascript is just hosed as far as reducing you anonymity set
  See: Gregory Fleischer, DEFCON 17: Attacking Tor at the Application Layer

DNS Leaks



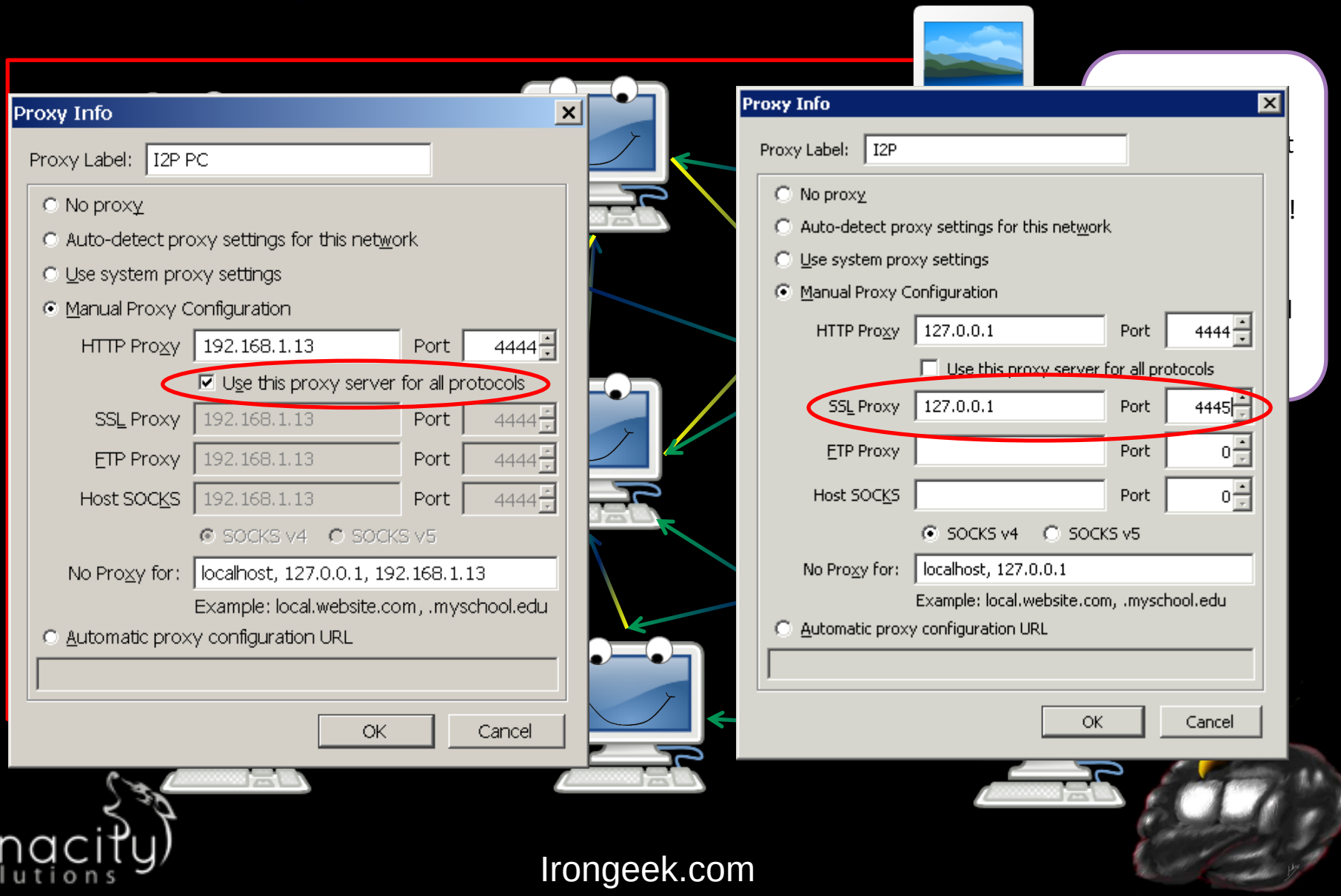
tenacity solutions

Irongeek.com

Mitigating DNS Leaks

- Sniff for traffic leaving your box on port 53. The libPcap capture filter:
  port 53
  should work in most cases.
- In Firefox, under about:config set network.proxy.socks_remote_dns to true
- Torbutton should help
- Other applications vary
- May have to firewall off 53 in some cases
- May want to edit torrc, and add:
  DNSPort 53
  AutomapHostsOnResolve 1
  Then set your box's DNS to point to 127.0.0.1

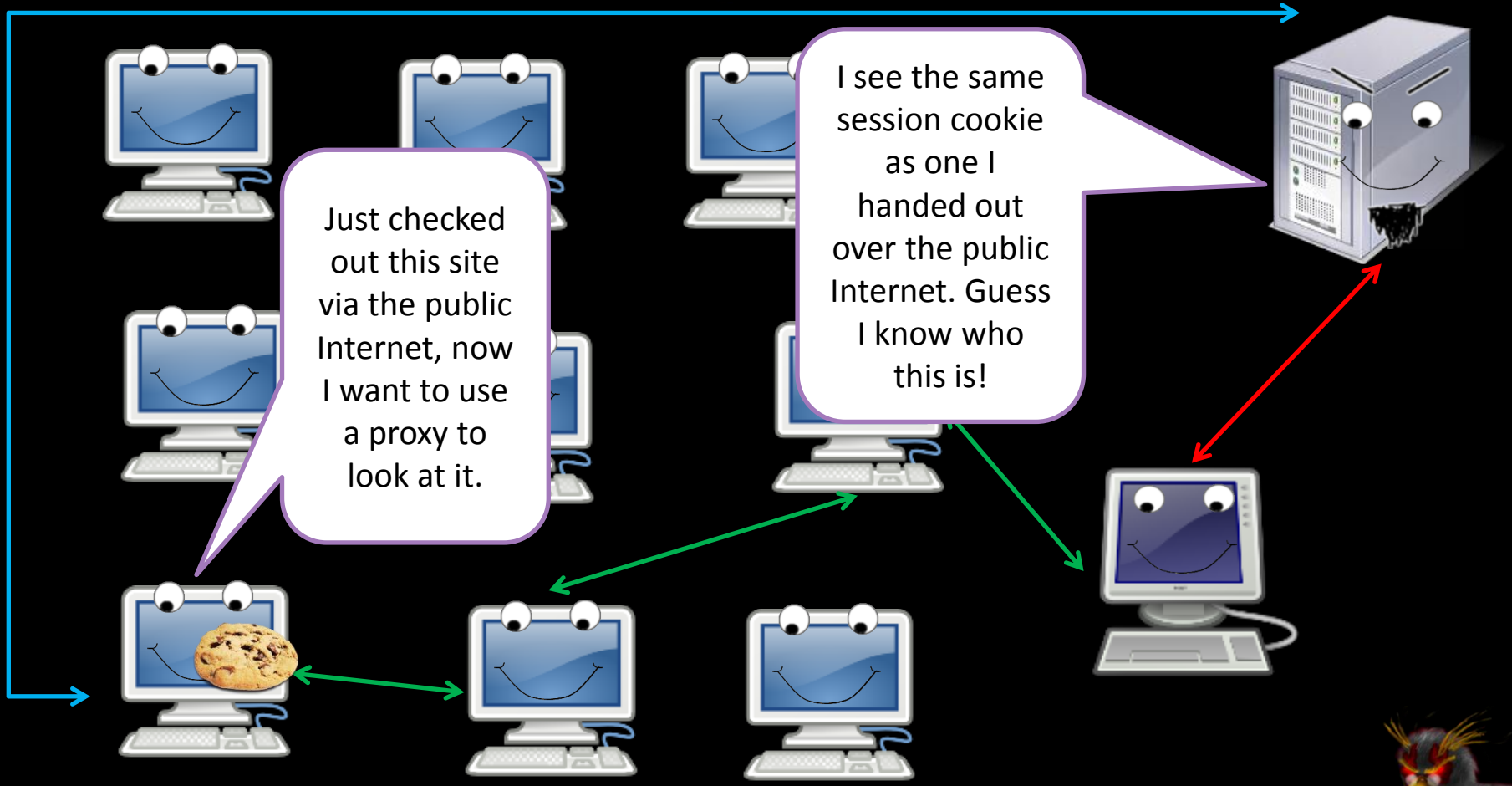
Grabbing content outside of the Darknet



tenacity solutions

Irongeek.com

Slightly Related: Cookies/Supercookies/Etc

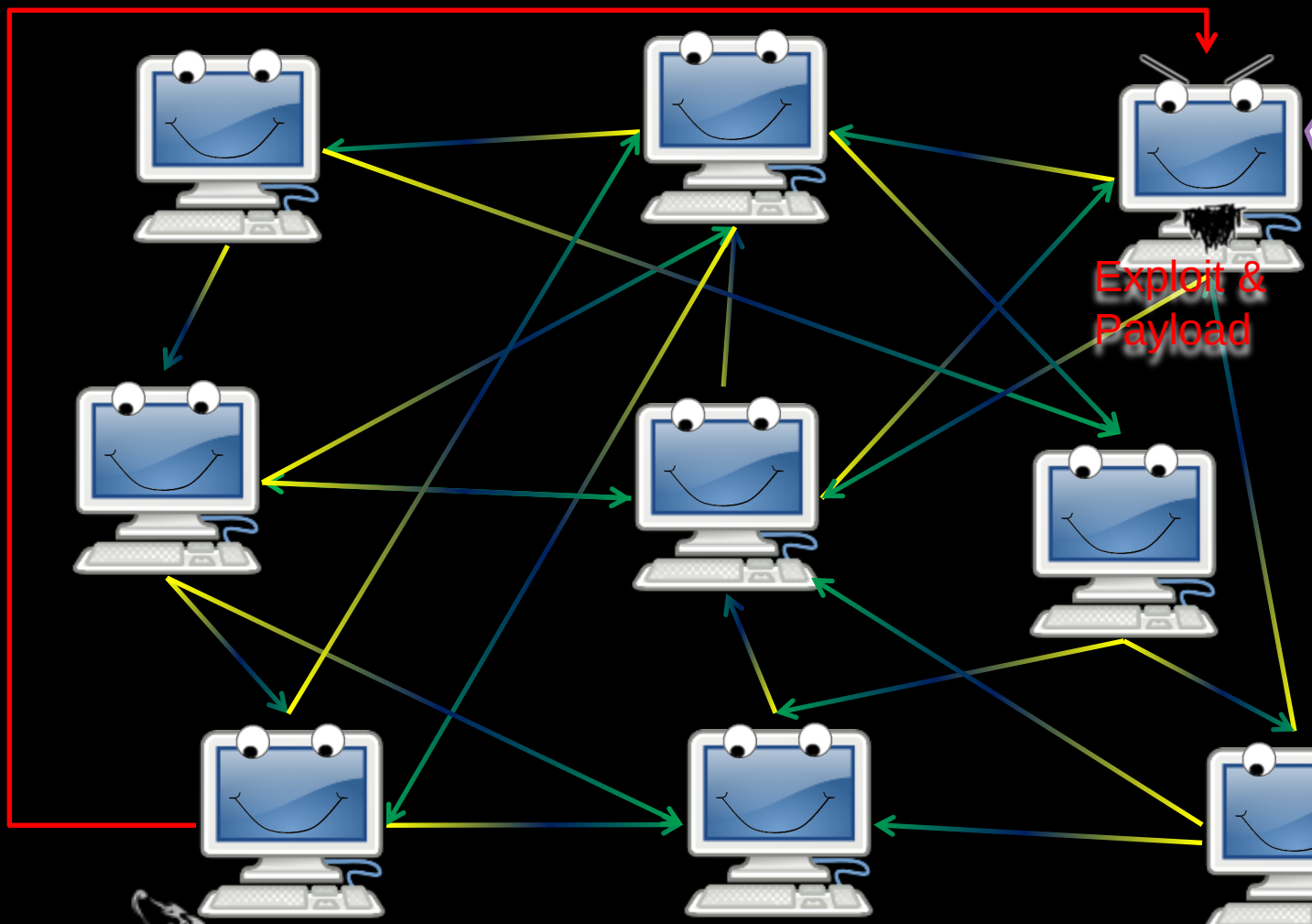


tenacity solutions

Cookie image from brainloc on sxc.hu via Wikipedia

Irongeek.com

Make hidden server contact you over public Internet

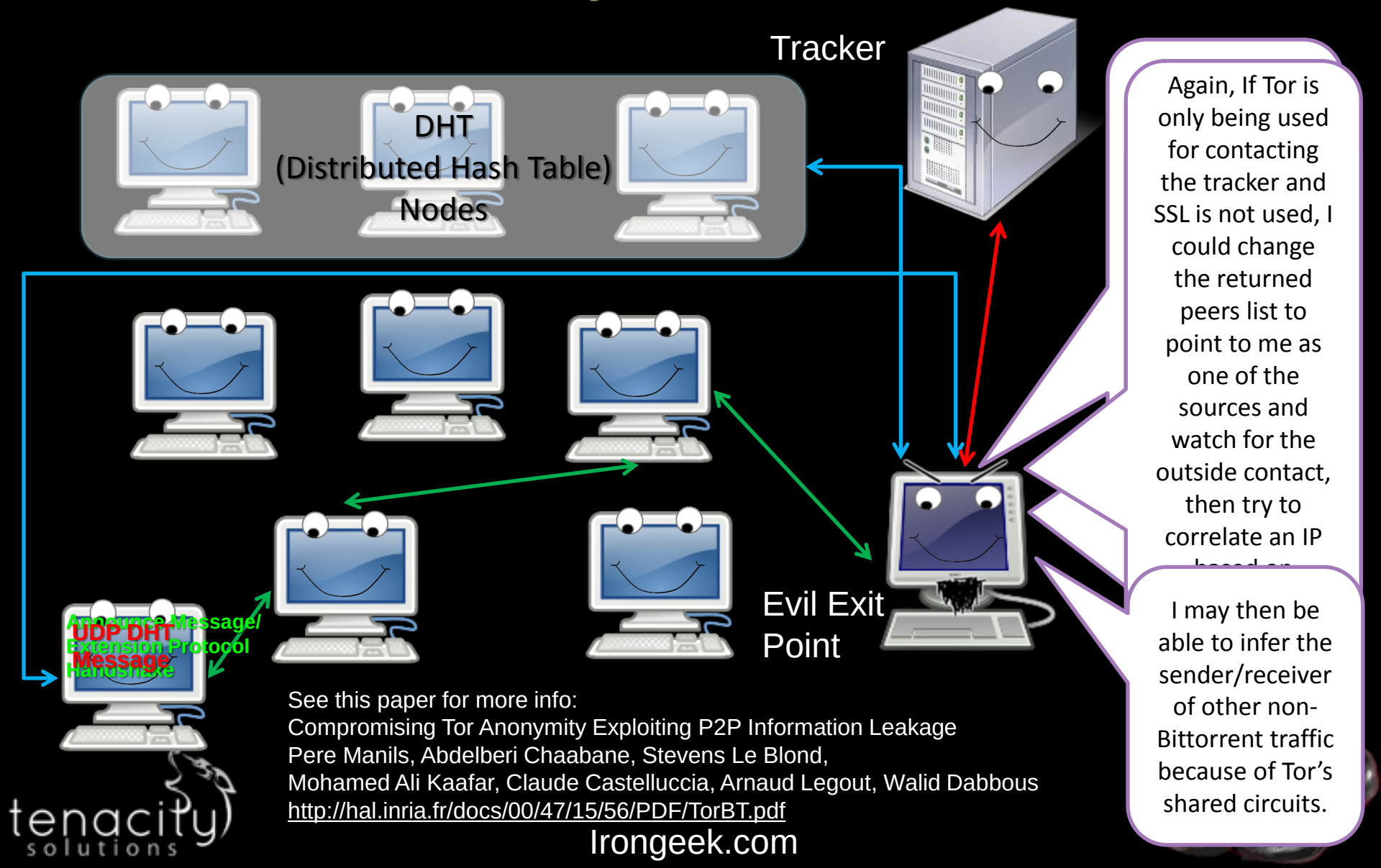


Let's see if the hidden server app is vulnerable to an exploit (buffer overflow/web app shell exec/etc).

Send a payload that contacts an IP I monitor.

tenacity solutions

Another example, Bittorrent Issues

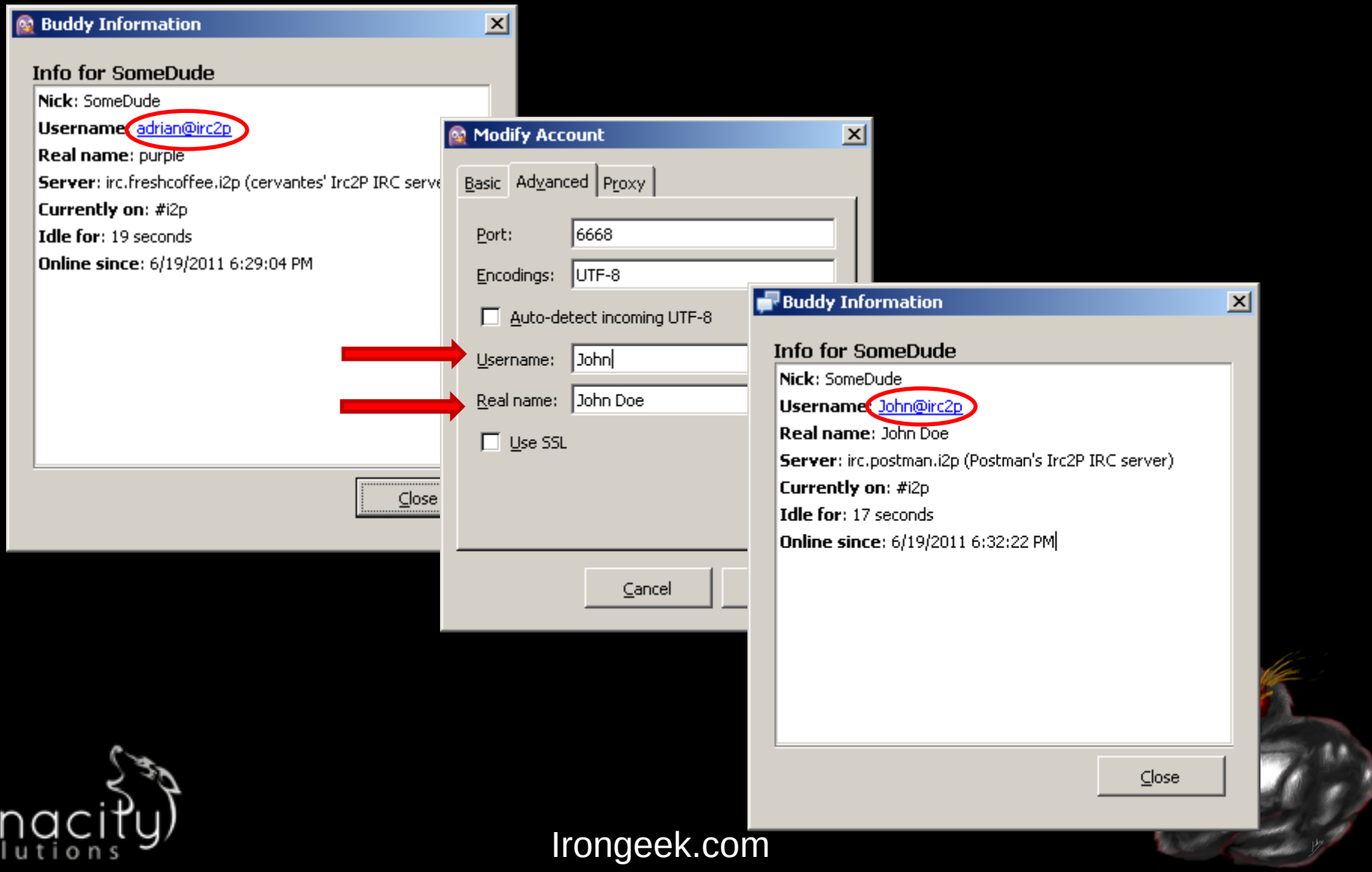


See this paper for more info:
Compromising Tor Anonymity Exploiting P2P Information Leakage
Pere Manils, Abdelberi Chaabane, Stevens Le Blond,
Mohamed Ali Kaafar, Claude Castelluccia, Arnaud Legout, Walid Dabbous
http://hal.inria.fr/docs/00/47/15/56/PDF/TorBT.pdf

tenacity solutions

Irongeek.com

Yet Another Example: IRC Ident



General Mitigations

Client wise:

- Make sure your browser is set to send all traffic though the darknet, or none at all
- Look into firewall rules
- Limit plugins used
- Use a separate browser
- Check against:
  http://decloak.net/
  http://panopticlick.eff.org/

Hidden server wise:

- Patch your stuff
- Don’t run on a box that routes to the Internet

ATTACKS ON CENTRALIZED RESOURCES/INFRASTRUCTURE ATTACKS/DoS ATTACKS

Overview

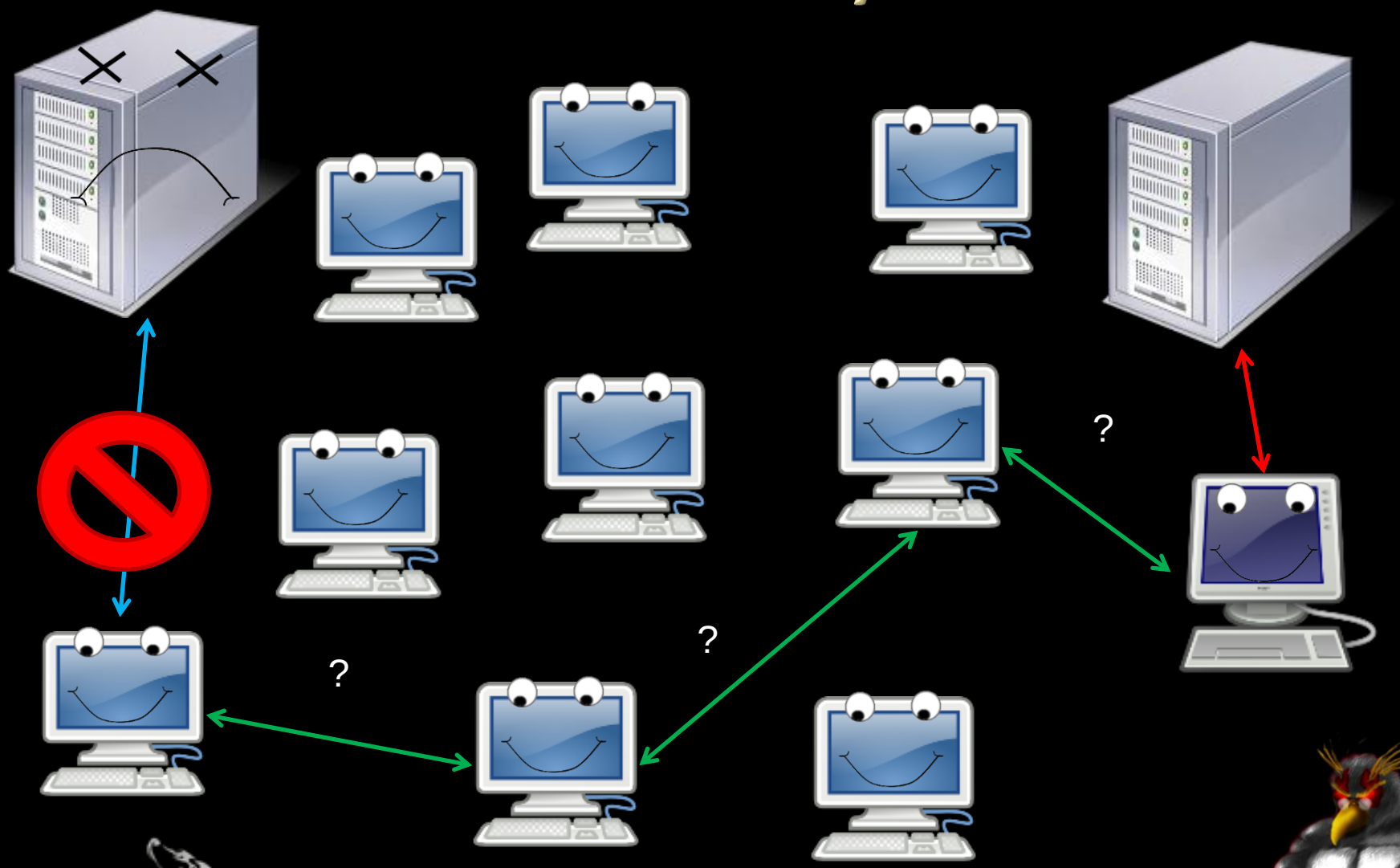
- Not so much against individual nodes, but the network in general
- Whole bunch of categories, not comprehensive:
  - Starvation attacks
  - Partition attacks
  - Flooding
- Standard DDoS attacks against resources inside and outside of the network (if going though the network) are likely to be soaked by other peers
- Shared known infrastructure can be a problem
- Total (or at least severe) blocking of the Internet

Incidents

- China blocked access to the core directory servers of Tor on September 25th 2009 https://blog.torproject.org/blog/tor-partially-blocked-china
- Other blocking of Internet access. (Egypt, Libya, Iran)

Tor Directory Server

DoS of directory servers



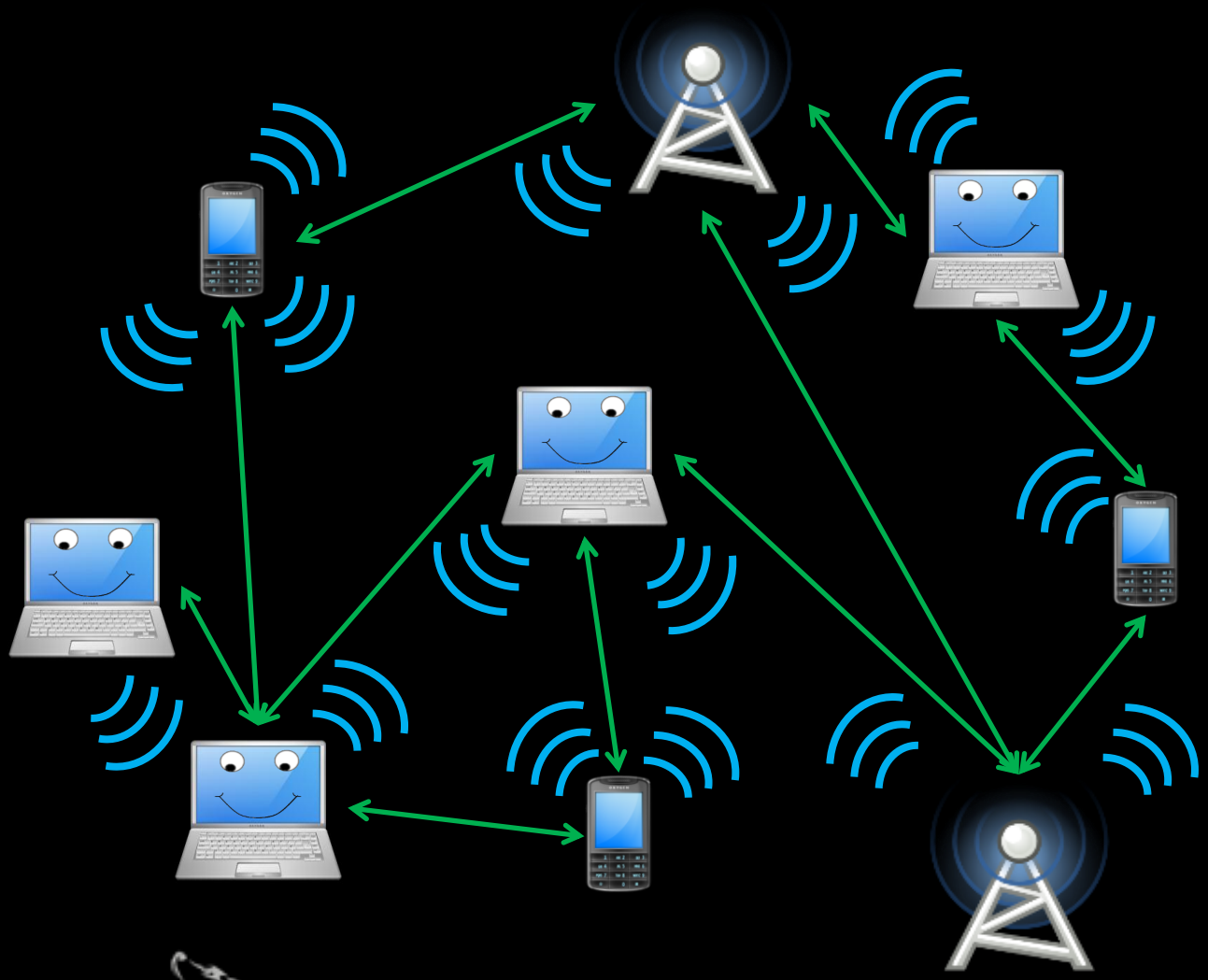
tenacity solutions

Irongeek.com

Mitigation

- Bridge nodes (Tor)
- Distributed infrastructure (I2P)
  - Taking out dev site would still be an issue
- Distributed Hash Table
- Protocol obfuscation
- Total/Severe blocking will take a bit more:
  (see next slide)

Mesh/Store and forward



tenacity solutions

For more info on mesh networks

- Needs a clear front runner for setting up such a system
- Wikipedia if nothing else
  http://en.wikipedia.org/wiki/Wireless_mesh_network
- Village Infrastructure in a Kit-Alpha (VIKA) Project
  http://www.cuwin.net/node/325
- U.S. Underwrites Internet Detour Around Censors
  http://www.nytimes.com/2011/06/12/world/12internet.html?_r=2&pagewanted=all

tenacity solutions

CLOCK BASED ATTACKS

Overview

- Some protocols allow you to check the remote system's clock
- Clock difference could be an issue
- Minor clock issues may need statistical analysis

Incidents

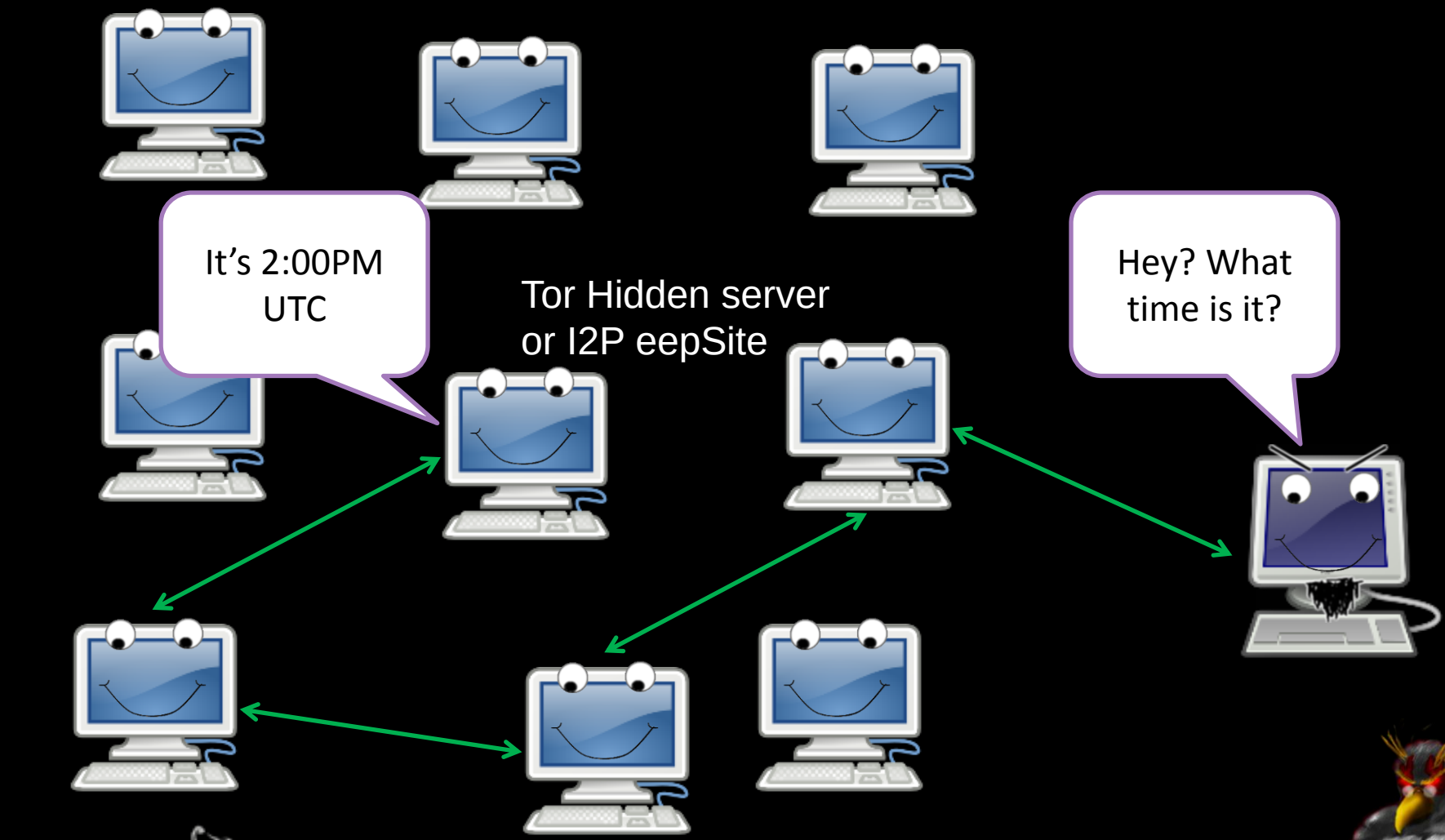
- For skew, see:
  Steven J. Murdoch, "Hot or Not: Revealing Hidden Services by their Clock Skew"
  University of Cambridge, Cambridge, 2006
  http://www.freehaven.net/anonbib/cache/HotOrNot.pdf

- I2P Clock differences in I2P
  http://www.irongeek.com/i.php?page=security/darknets-i2p-identifying-hidden-servers

Clock Differences

Time Difference	Retrieval Time	Host	Header
40.417	0.436	89.31.112.91	Apache/2.2.13 (Linux/SUSE)
50.294	10.549	medosbor.i2p	Apache/2.2.13 (Linux/SUSE)
3.418	0.35	85.229.85.244	Apache/2.2.15 (Debian)
4.325	5.059	jonatan.walck.i2p	Apache/2.2.15 (Debian)
-4325.58	0.353	84.55.73.228	Apache/2.2.3 (CentOS)
-4321.66	8.946	ipredia.i2p	Apache/2.2.3 (CentOS)
4488.434	0.702	130.241.45.216	Apache/2.2.9 (Debian) PHP/5.2.6-1+lenny8 with Suhosin-Patch
4490.365	4.894	error.i2p	Apache/2.2.9 (Debian) PHP/5.2.6-1+lenny8 with Suhosin-Patch
2.407	4.89	bolobomb.i2p	Apache/2.2.9 (Debian) PHP/5.2.6-1+lenny9 with Suhosin-Patch mod_ssl/2.2.9 OpenSSL/0.9.8g
2.421	0.091	83.222.124.19	Apache/2.2.9 (Debian) PHP/5.2.6-1+lenny9 with Suhosin-Patch mod_ssl/2.2.9 OpenSSL/0.9.8g
3.43	0.282	188.40.181.33	lighttpd/1.4.22
5.366	2.901	docs.i2p2.i2p	lighttpd/1.4.22
6.274	3.673	zzz.i2p	lighttpd/1.4.22
53.415	0.26	93.174.93.93	Microsoft-IIS/6.0
54.404	3.92	colombo-bt.i2p	Microsoft-IIS/6.0
3.287	0.531	www.i2p2.i2p	nginx/0.6.32
3.429	0.285	46.4.248.202	nginx/0.6.32
11.323	8.989	lurker.i2p	nginx/0.7.65
12.433	8.882	178.63.47.16	nginx/0.7.65

Clock Issues



Mitigation

- Attack can be hard to pull off because of network jitter
- Set clocks with a reliably and often used NTP server
- Some mitigation may take place in the darknet protocol itself

METADATA IN FILES

tenacity solutions

Irongeek.com

Overview

- Matadata is data about data
- Just a few files types that contain metadata
  - JPG
    EXIF (Exchangeable image file format)
    IPTC (International Press Telecommunications Council)
  - PDF
  - DOC
  - DOCX
  - EXE
  - XLS
  - XLSX
  - PNG
  - Too many to name them all
- Things stored: User names, edits, GPS info, network paths, MAC addresses in odd cases. It all depends on the file format.

Incidents: Pwned by Metadata

Cat Schwartz
Is that an unintended thumbnail in your EXIF data, or are you just happy to see me?

Dennis Rader (BTK Killer)
Metadata in a Word DOC he sent to police had the name of his church, and last modified by “Dennis” in it.

Darkanaku/Nephew chan
A user on 4chan posts a pic of his semi-nude aunt taken with an iPhone, Anonymous pulls the EXIF GPS info from the file and hilarity ensues.
More details can be on the following VNSFW site:
~~http://encyclopediadramatica.com/User:Darkanaku/Nephew_chan~~
http://web.archive.org/web/20090608214029/http://encyclopediadramatica.com/User:Darkanaku/Nephew_chan

tenacity solutions

Irongeek.com

Mitigation

- Well, clean out the metadata, duh!
- Apps vary on how to do it

LOCAL ATTACKS

(at this point, it is already probably a lost cause)

Overview

- If they have access to the local box, your hosed
- Comes down to mostly traditional forensics
  - Data on hard drive
  - Cached data and URLs
  - Memory Forensics

Mitigations

- Anti-forensics http://www.irongeek.com/i.php?page=videos/anti-forensics-occult-computing
- Live CD/USB, but see Andrey Case's work: https://media.blackhat.com/bh-dc-11/Case/BlackHat_DC_2011_Case_De-Anonymizing_Live_CDs-wp.pdf
- Full hard drive encryption

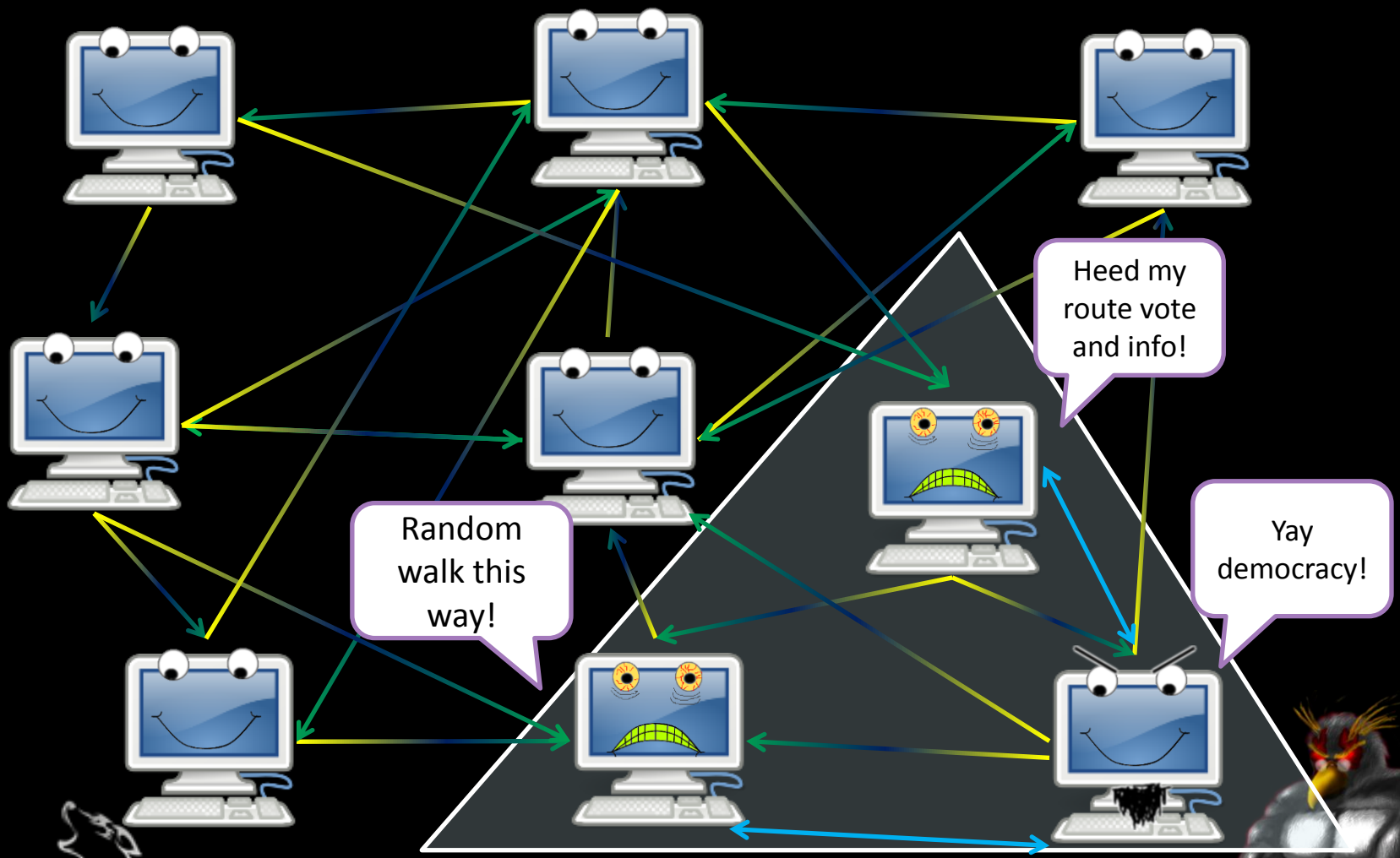
SYBIL ATTACKS

Sock puppetry

Overview

- Ever heard of Sybil attacks?
- Think sock puppet, one entity acting as many
- May allow for control of routing, elections, etc.
- Makes many of the other attacks easier

Sock puppetry/Sybil



Mitigation

No absolute fixes

- Make it cost more to have nodes (hashcash)
- IP restrictions:
  Both Tor and I2P restrict peering between IPs on the same /16
- Central infrastructure may be more resilient against Sybil attacks (but has other issues)
- Peering strategies
- SybilLimit/SybilGuard/SybilInfer

TRAFFIC ANALYSIS ATTACKS

First/Last in chain attacks

Tagging attacks

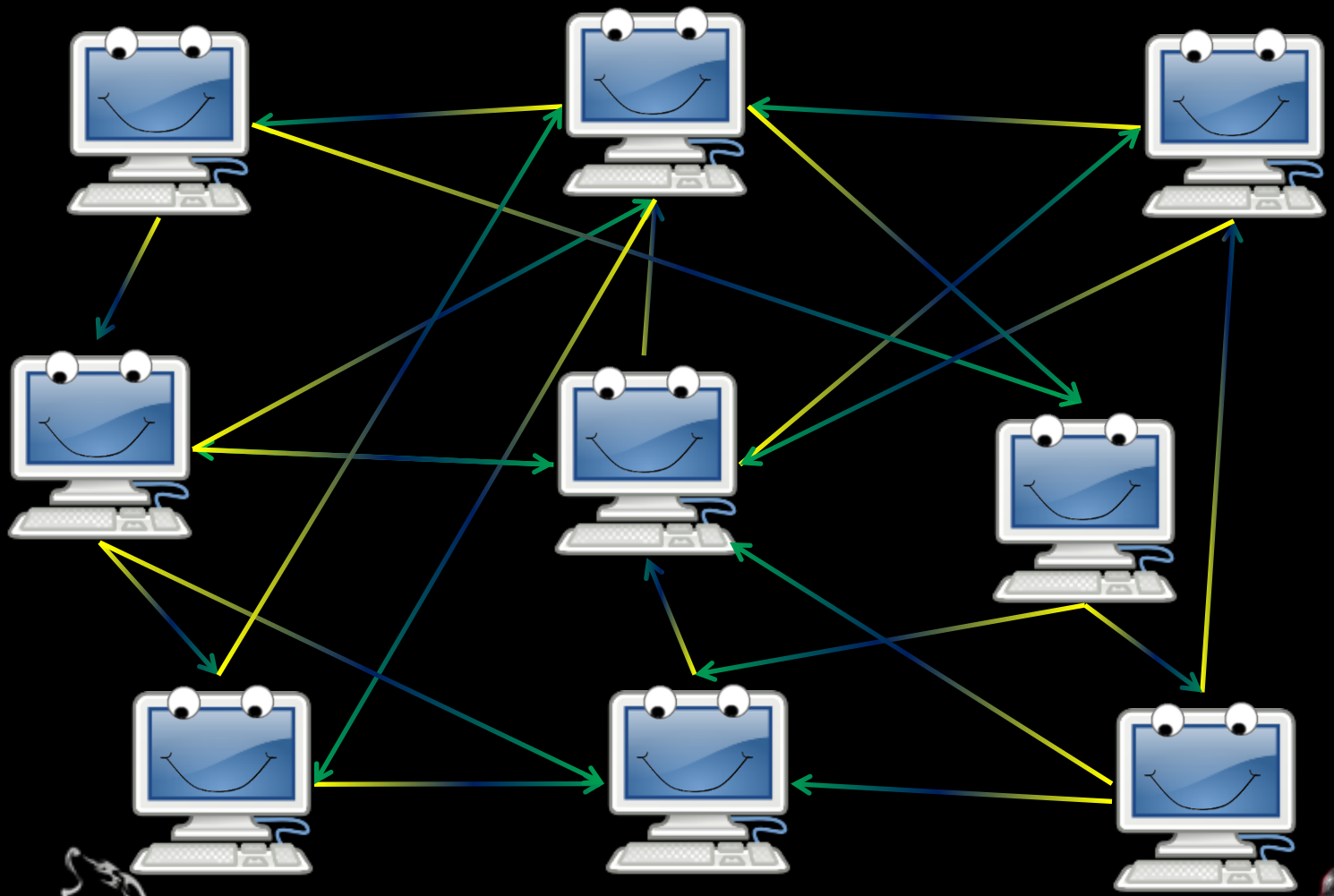
Timing attacks

tenacity solutions

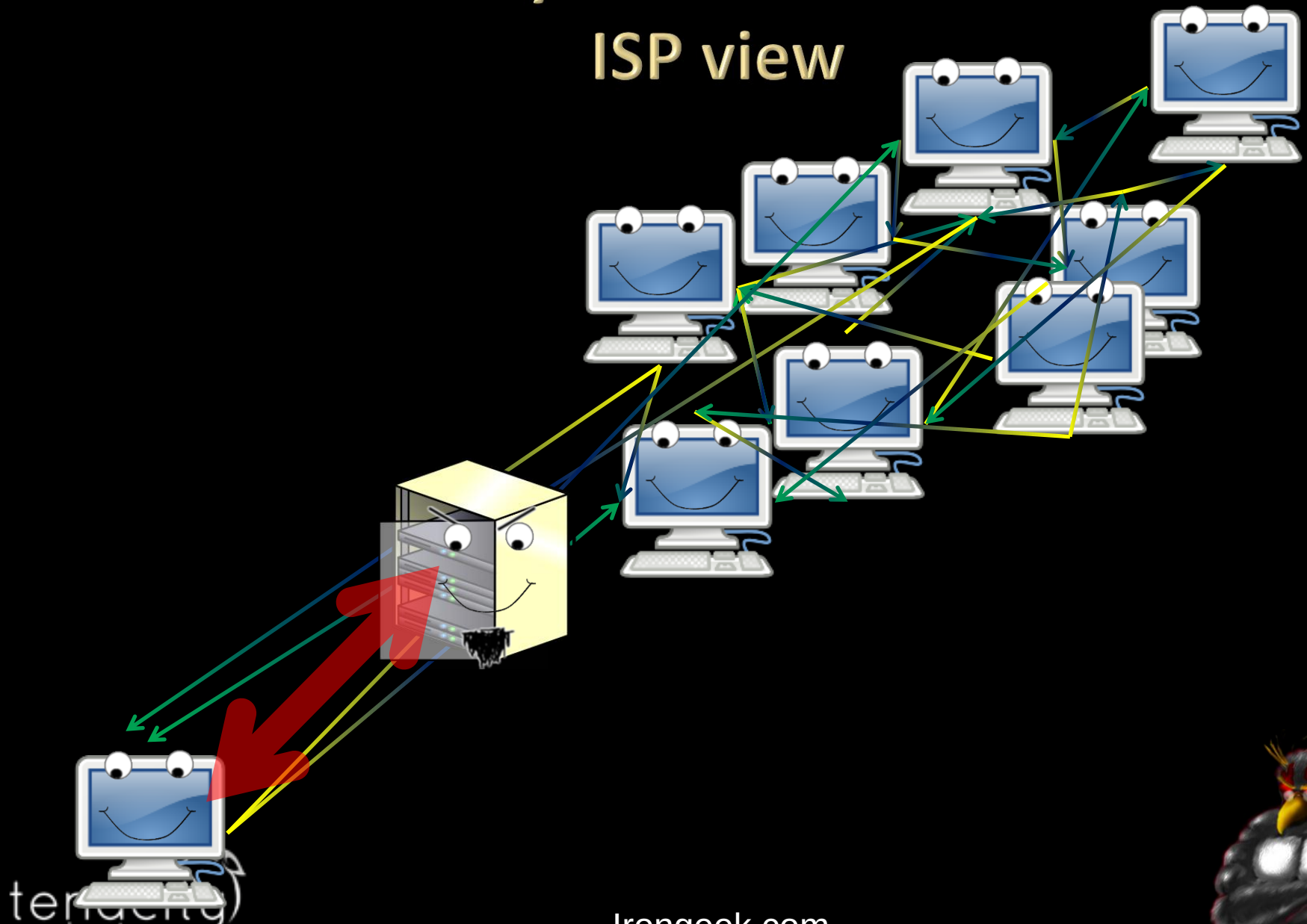
Overview

- There's much focus on this in academia, but I imagine application layer flaws are more likely to snag someone
- So many subtle variation on profiling traffic
- Could be:
  - Timing of data exchanges
  - Amount of traffic
  - Tagging of traffic by colluding peers
- Generally takes a powerful adversary
- Hard to defeat in "low latency" networks

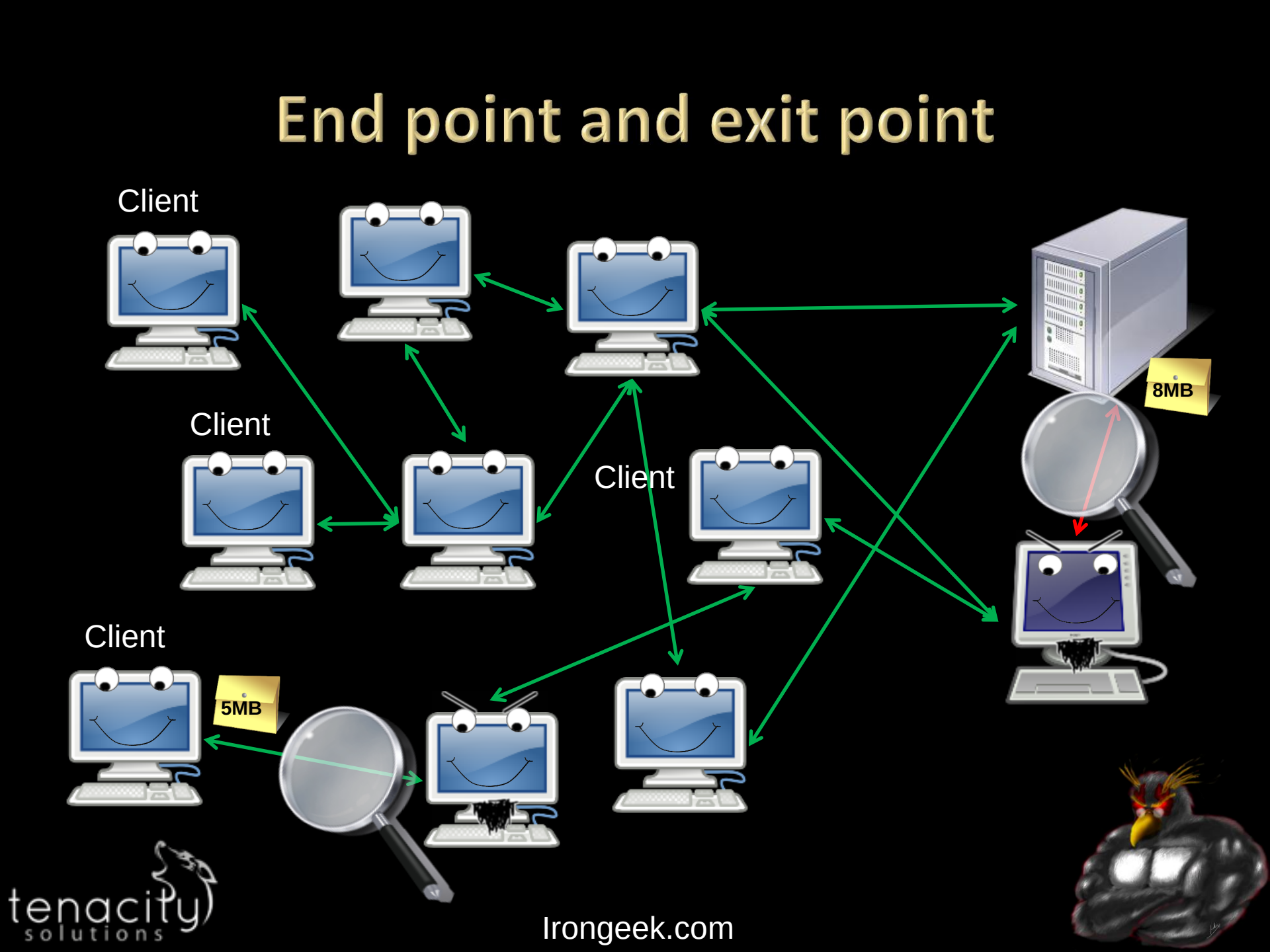
I2P one-way tunnel mesh network: Logical view



I2P one-way tunnel mesh network: ISP view



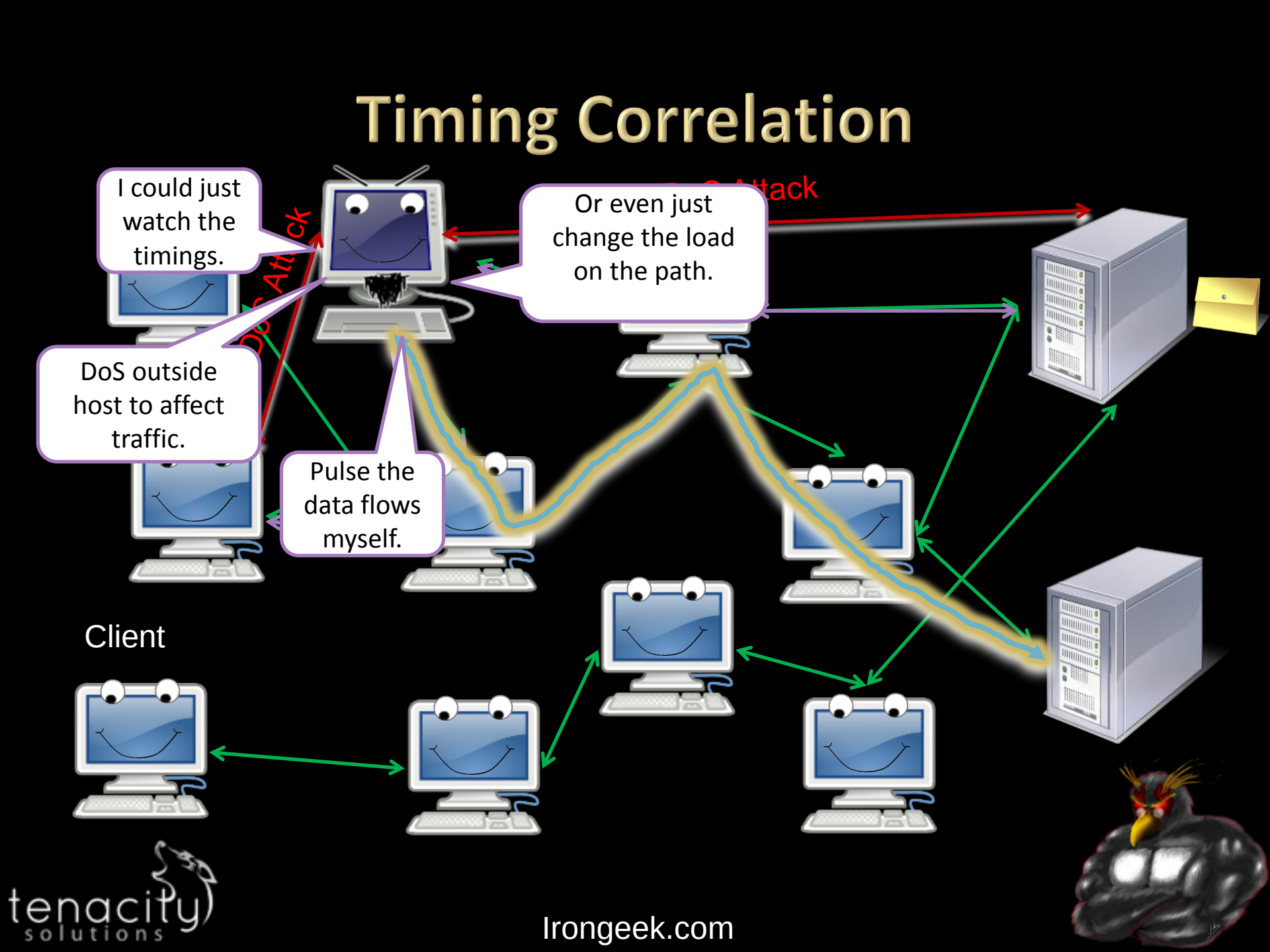
End point and exit point



tenacity solutions

Irongeek.com

Timing Correlation



tenacity solutions

Irongeek.com

Mitigation

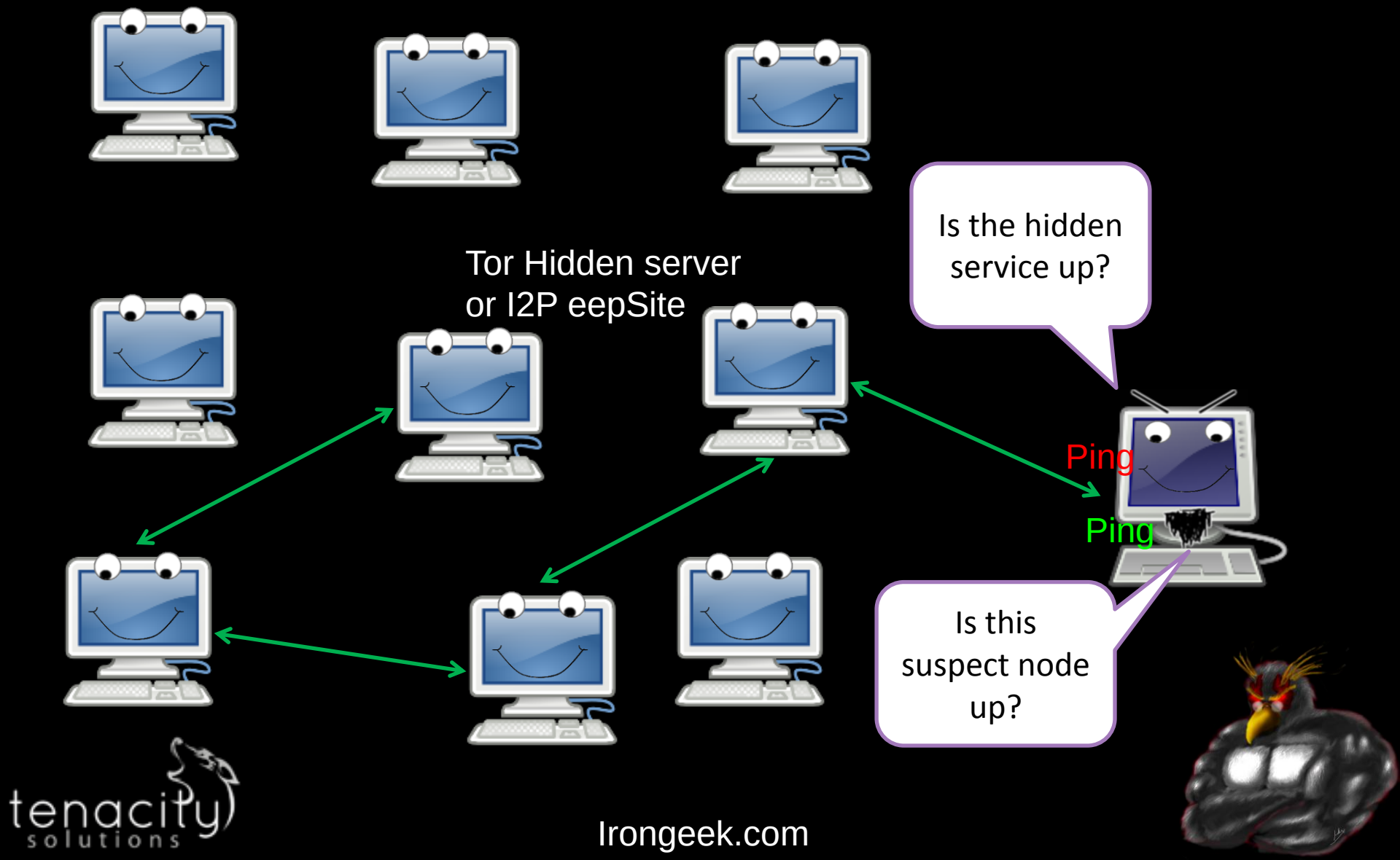
- More routers
- More cover traffic
  (smaller needle in a larger haystack)
- Entry Guards for first hop
- One way tunnels
- Short lived tunnels may help, ends of tunnels act as rendezvous points
- Better peer profiling
- Signing of the data
- Fixed speeds
- Padding and Chaff
- Non-trivial delays and Batching

INTERSECTION/CORRELATION ATTACKS

Overview

- Could be as simple as knowing who is up when a hidden service can be accessed
- Techniques can be used to reduce the search set
- Application flaws and information leaks can narrow the anonymity set
- Harvesting attacks

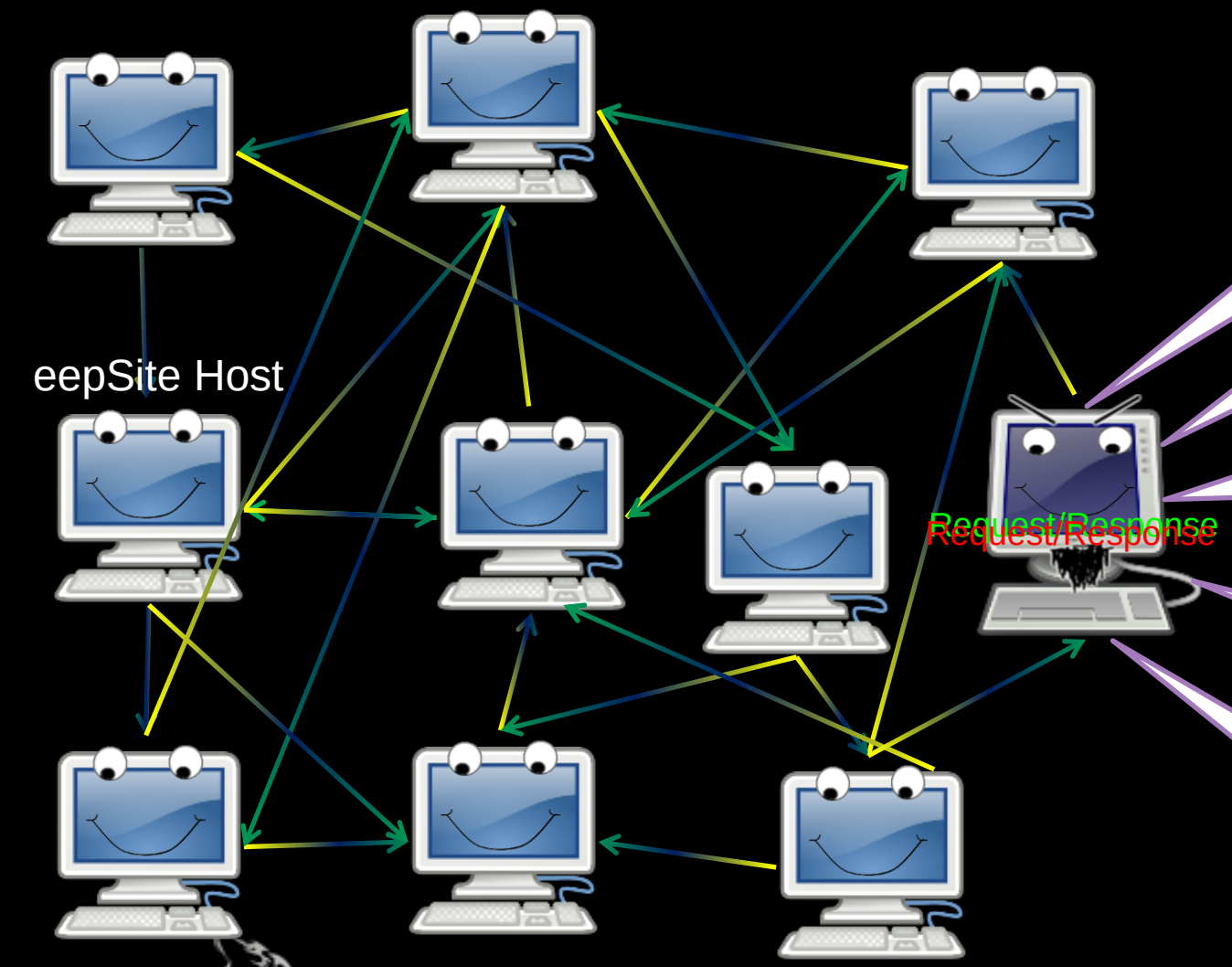
Correlation



tenacity solutions

Irongeek.com

Cut down needed checks



1. What server software are you running an eepSite on?

2. Harvest as many peer IPs as I can.

3. Is there a web service on the public facing IP using the same daemon?

4. Does it respond to the same Vhost request?

5. If so, yippy! Found you!

tenacity solutions

Irongeek.com

Mitigation

- More nodes
- Give less data that could be used to reduce the anonymity set
- Make harvesting/scrapping attacks harder
- Checkout “De-anonymizing I2P” paper and talk I’ll link to later

Links

- Selected Papers in Anonymity
  http://www.freehaven.net/anonbib/
- I2P's Threat Model Page
  http://www.i2p2.de/how_threatmodel.html
- General Darknets Talk
  http://www.irongeek.com/i.php?page=videos/aide-winter-2011#Cipherspace/Darknets:_anonymizing_private_networks
- De-anonymizing I2P
  http://www.irongeek.com/i.php?page=security/darknets-i2p-identifying-hidden-servers
  http://www.irongeek.com/i.php?page=videos/identifying-the-true-ip-network-identity-of-i2p-service-hosts-talk-adrian-crenshaw-blackhat-dc-2011

Thanks

- Conference organizers for having me
- Tenacity for helping get me to Defcon
- By buddies from Derbycon and the ISDPodcast
- Open Icon Library for some of my images http://openiconlibrary.sourceforge.net

Events

- DerbyCon 2011, Louisville Ky
  Sept 30 - Oct 2
  http://derbycon.com
- Louisville Infosec
  http://www.louisvilleinfosec.com
- Other Cons:
  http://skydogcon.com
  http://dojocon.org
  http://hack3rcon.org
  http://phreaknic.info
  http://notacon.org
  http://outerz0ne.org

QUESTIONS?

42

tenacity solutions

Irongeek.com