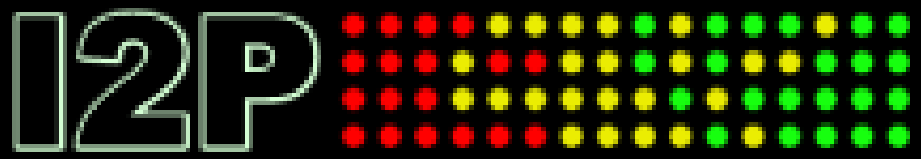
PROJECT PROPOSAL: LOCATING I2P SERVICES VIA LEAKS ON THE APPLICATION LAYER

Adrian Crenshaw

A little background…

Darknets

- There are many definitions, but mine is “anonymizing private networks ”
- Use of encryption and proxies (some times other peers) to obfuscate who is communicating to whom



I2P

Invisible Internet Project

(in a nutshell)

Especially as compared to Tor

Overview

- **Who?**

  I2P developers, started by Jrandom.
  http://www.i2p2.de/

- **Why?**

  To act as an anonymizing layer on top of the Internet

- **What?**

  Mostly other web sites on I2P (eepSites), but the protocol allows for P2P (iMule, i2psnark), anonymous email and public Internet via out proxies.

- **How?**

  Locally ran proxies that you can connect to and control via a web browser. These connect other I2P routers via tunnels. Network information is distributed via a DHT know as NetDB.

Layout

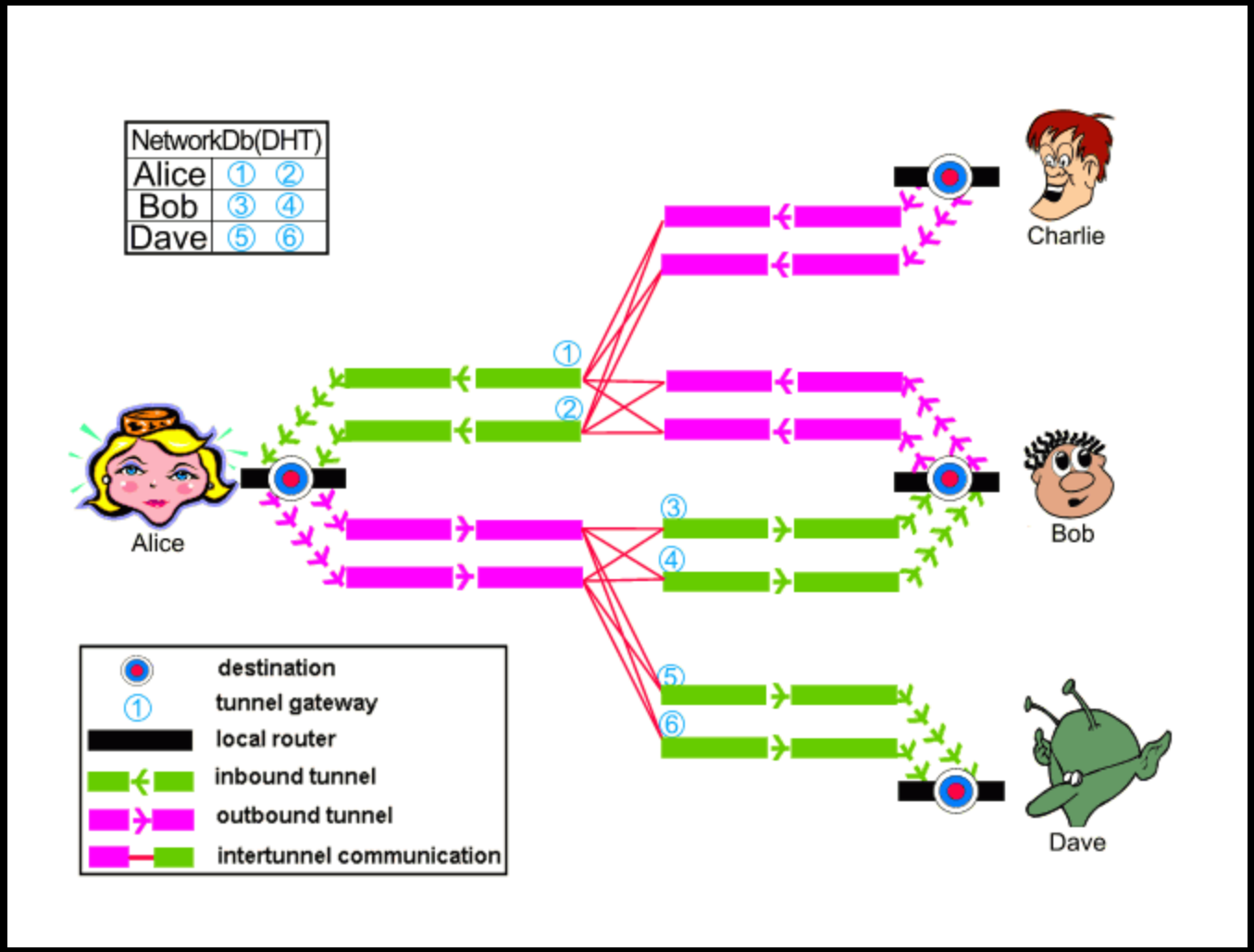
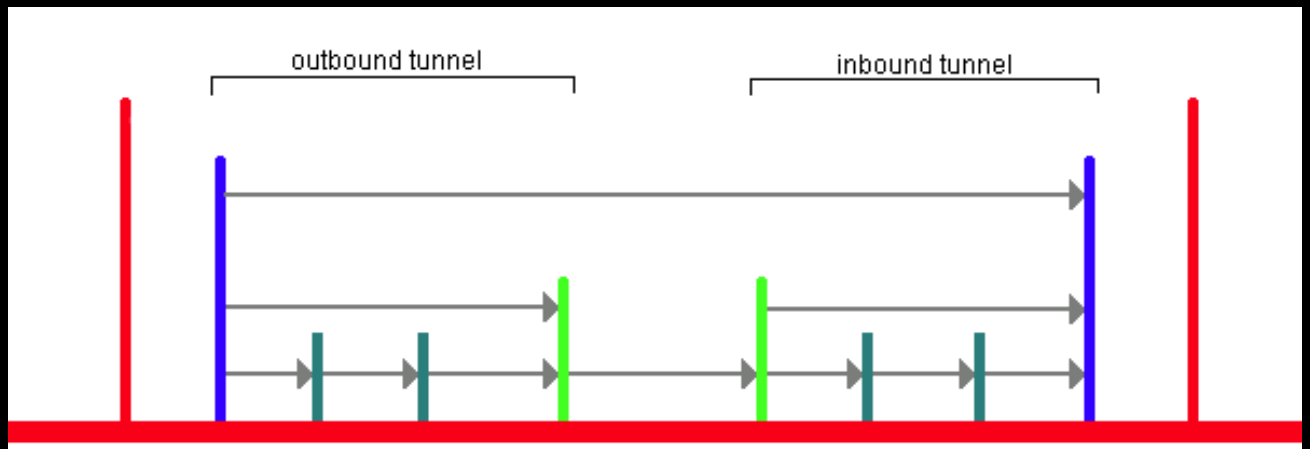


Image from http://www.i2p2.de/how_intro

Encryption Layers

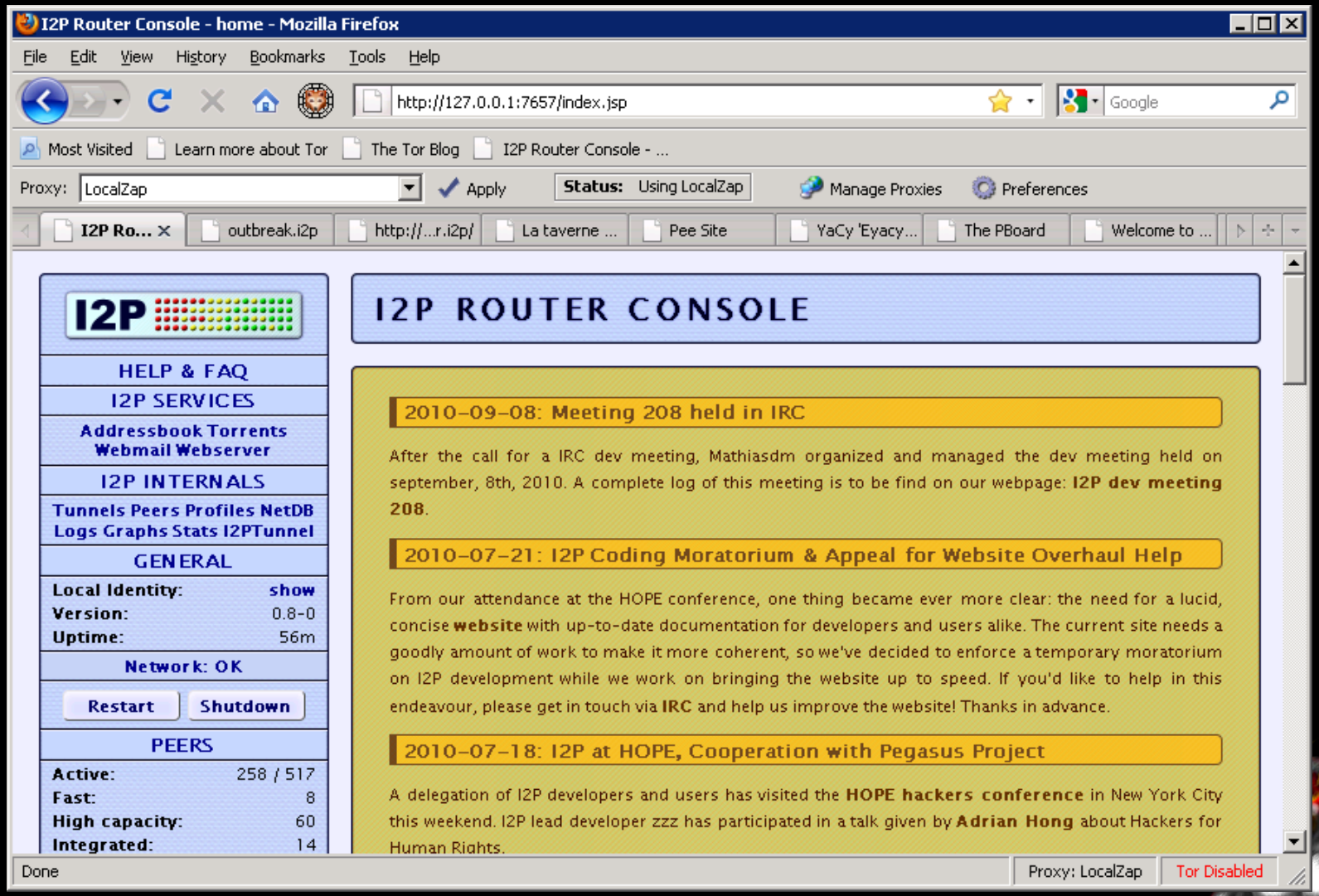
- EIGamal/SessionTag+AES from A to H
- Private Key AES from A to D and E to H
- Diffie–Hellman/Station-To-Station protocol + AES



		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/

What does it look like to the user?



http://Irongeek.com

Naming and Addresses

- Details
  http://www.i2p2.de/naming.html
- 516 Character Address

```
-KR6qyfPWXoN~F3UzzYSMIsaRy4udcRkHu2Dx9syXSz
UQXQdi2Af1TV2UMH3PpPuNu-GwrqihwmLSkPFg4fv4y
QQY3E10VeQVuI67dn5vlan3NGMsjqxoXTSHHt7C3nX3
szXK90JSoO~tRMDl1xyqtKm94-RpIyNcLXofd0H6b02
683CQIjb-7JiCpDD0zharm6SU54rhdisIUVXpi1xYgg
2pKVpssL~KCp7RAGzpt2rSgz~RHFsecqGBeFwJdiko-
6CYW~tcBcigM8ea57LK7JjCFVhOoYTqgk95AG04-hfe
hnmBtuAFHWklFyFh88x6mS9sbVPvi-am4La0G0jvUJw
9a3wQ67jMr6KWQ~w~bFe~FDqoZqVXl8t88qHPIvXelv
Ww2Y8EMSF5PJhWw~AZfoWOA5VQVYvcmGzZIEKtFGE7b
gQf3rFtJ2FAtig9XXBsoLisHbJgeVb29Ew5E7bkwxvE
e9NYkIqvrKvUAt1i55we0Nkt6xlEdhBqg6xXOyIAAAA
```

- SusiDNS Names
  something.i2p
- Hosts.txt and Jump Services
- Base32 Address
  {52 chars}.b32.i2p
  rjxwbsw4zjhv4zsplma6jmf5nr24e4ymvvbycd3swgiinbvg7oga.b32.i2p

I2P Pros and Cons

Pros

- Lots of supported applications
- Can create just about any hidden service if you use SOCKS5 as the client tunnel
- Eepsites somewhat faster compared to Tor Hidden Services (Subjective, I know)
- No central point of failure
  (Example: What happened to Tor when China blocked access to the core directory servers on September 25th 2009)

Cons

- Limited out proxies
- Sybil attacks a little more likely

Approach

1. Spidering the content of the eepSite for related sites.
2. Using tools like Nikto to find directories and files that reveal server information.
3. HTTP headers may be returned by the sites that reveal information.
4. Putting bait in logs via the user agent string that may make the administrator of the site visit a tracking page unproxied.
5. ~~See if reverse DNS lookups done by the webserver when it generates logs give away its true IP.~~
6. Consult with security and privacy community at large for more ideas.
7. Flesh out some of the attacks listed in the threat model page.
8. Review the server and client proxy code for flaws.
9. Look at the Tor change log and see if any bugs were fixed that may still exist in I2P.

Thanks to ZZZ for suggesting the last three points.

Challenges

1. Communications with the eepSites is normally done via an HTTP proxy. This restricts my attack options somewhat.
2. Perhaps because of point one, many of the tools I have experimented with so far have a tendency to give false results or hang while working on spidering an eepSite.
3. While spidering I need to be careful not to download contraband onto my own system.

Improvements/Deliverables

1. Clearer examples of how leaked information can be found.
2. A concentration on I2P instead of Tor.
3. A concentration on the application layer instead of the network or transport layers.
4. Real world tests on systems that have been implemented for more than just academic purposes.
5. Less reliance on esoteric attack vectors.

Schedule

Week of Oct 5:

Research deeper into I2P and how it works.

Evaluate web application fingerprinting tools.

Week of Oct 12:

Give project proposal presentation.

Continue work from week one.

Look into developing or modifying existing tools to work better with I2P.

Week of Oct 19:

Run extensive tests with tools to see what information can be found.

Week of Oct 26:

Continue testing tools and collecting data on eepSites. This will continue up until the final draft of the project paper.

Week of Nov 2:

Parse collected data into a format that can be explained to others.

Week of Nov 9:

Work on status report.

Week of Nov 16:

Turn in status report and consider new directions to go.

Week of Nov 23:

Implement changes based on status report feedback.

Week of Nov 30:

Polish draft of final project report so it can be tuned in next week.

Week of Dec 7:

Turn in final project report and begin work on presentation.

Week of Dec 14:

Give final project presentation.

http://Irongeek.com

QUESTIONS?

42

Project Page:
http://www.irongeek.com/i.php?page=security/i2p-identify-service-hosts-eepsites&mode=print

Installing:
http://www.irongeek.com/i.php?page=videos/getting-started-with-the-i2p-darknet