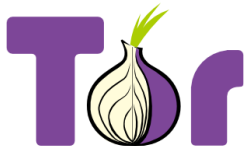


# NNEDV ToT9

Andrew Lewman  
andrew@torproject.org

08 August 2011



**TorProject.org**

George Orwell

nineteen

eighty-four

a novel

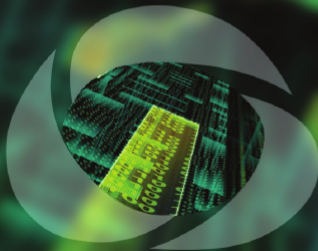


*Who controls the past, controls the future: who controls the present controls the past*

— George Orwell, *Nineteen Eighty Four*, 1949

Internet Surveillance is getting more advanced

If You Can See It  
You Can **Monetize It**



Evolved DPI – See what's flowing through your network

# Internet Surveillance is getting more advanced

```
|0.541 | | https > 50936 [SYN,
| | (50936) <-----> (443)
|0.541 | | 50936 > https [ACK]
| | (50936) -----> (443)
|0.542 | | Client Hello
| | (50936) -----> (443)
|1.030 | | https > 50936 [ACK]
| | (50936) <-----> (443)
|1.033 | | Server Hello,
| | (50936) <-----> (443)
|1.124 | | 50936 > https [ACK]
| | (50936) -----> (443)
|2.079 | | [TCP Previous segme
| | (50936) <-----> (443)
|2.079 | | [TCP Dup ACK 12#1]
| | (50936) -----> (443)
|5.563 | | [TCP Retransmission
| | (50936) <-----> (443)
|5.563 | | 50936 > https [ACK]
| | (50936) -----> (443)
|6.008 | | [TCP Retransmission
| | (50936) <-----> (443)
|6.008 | | 50936 > https [ACK]
| | (50936) -----> (443)
|16.025 | | Client Key Exchange
| | (50936) -----> (443)
|17.533 | | [TCP Retransmission
| | (50936) -----> (443)
|20.735 | | [TCP Retransmission
| | (50936) -----> (443)
|21.127 | | [TCP Previous segme
| | (50936) <-----> (443)
|26.447 | | 50936 > https [FIN,
| | (50936) -----> (443)
|26.743 | | Encrypted Alert
| | (50936) <-----> (443)
|26.743 | | 50936 > https [RST]
| | (50936) -----> (443)
```

# Internet Surveillance is getting more advanced

## 'Comodo Hacker' Says He Acted Alone

**The plot thickens: In an effort to back up his claims, alleged hacker dumps apparent evidence of pilfered database from breached Comodo reseller, as well as Mozilla add-on site certificate**

By [Kelly Jackson Higgins](#) [InformationWeek](#)

April 09, 2011 12:00 AM

Comodo, a website certificate authority, revealed that nine SSL certificates were issued for fraudulent websites posing as domains for high-profile sites. Security researchers hope the incident will call attention to a certificate process they say is riddled with holes.

# Internet Surveillance is getting more advanced

## US company 'helped' Egypt block web

**Egypt's crackdown on web users allegedly aided by US company's product.**

Last Modified: 06 Feb 2011 03:23 GMT



Email Article



Print Article



Share Article



Send Feedback

When Egypt's uprising began nearly two weeks ago, there was a near-total internet blackout.

But exactly how was access cut off?

An American advocacy group called Free Press says it has uncovered a link to a California-based technology company that allegedly sold the Egyptian government equipment allowing it to track online activity.

Al Jazeera's Rob Reynolds reports.





## The Tor Project, Inc.

501(c)(3) non-profit organization dedicated to the research and development of technologies for online anonymity and privacy



Tor hides communication patterns by relaying data through volunteer servers

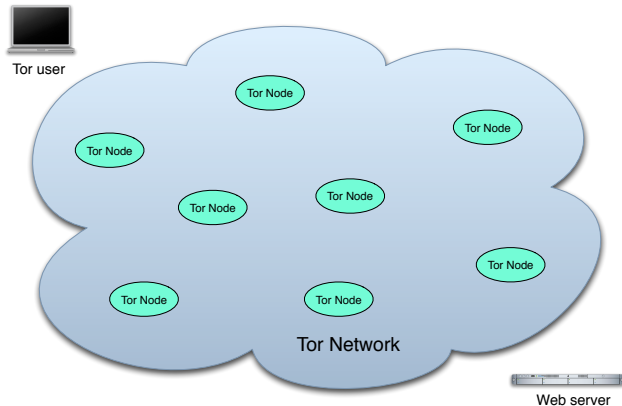
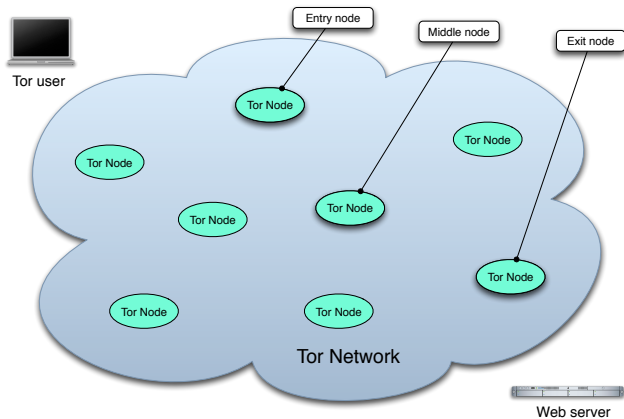


Diagram: Robert Watson

# Tor hides communication patterns by relaying data through volunteer servers



# Tor hides communication patterns by relaying data through volunteer servers

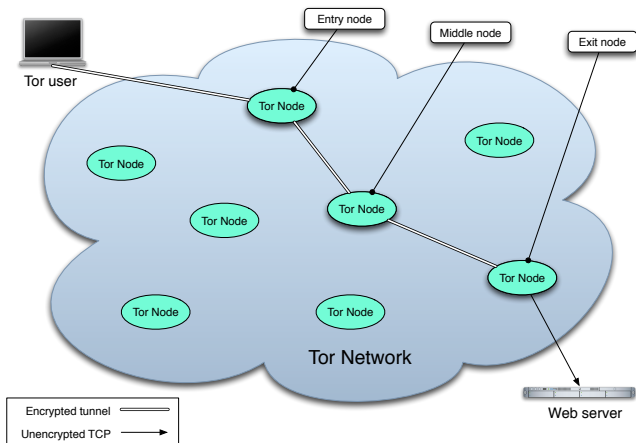
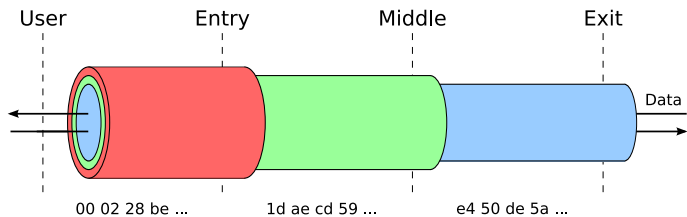


Diagram: Robert Watson

# Tor hides communication patterns by relaying data through volunteer servers



Thanks!

Visit <https://www.torproject.org/> for  
more information, links, and ideas.

## Copyright & Sources

- ▶ Internet surveillance, second image:  
<http://www.informationweek.com/news/security/attacks/229400850>
- ▶ Internet surveillance, third image: Al Jazeera, February 2011
- ▶ spring is in the air, Paco Pomet, <http://pacopomet.wordpress.com/>