Tor Performance and Security

Can we be anonymous at scale ?

Muhammad F. R. Wani

Department of Computer Science
Indraprashta Institute *of*
Information Technology Delhi

Term Paper Presentation, April 2017

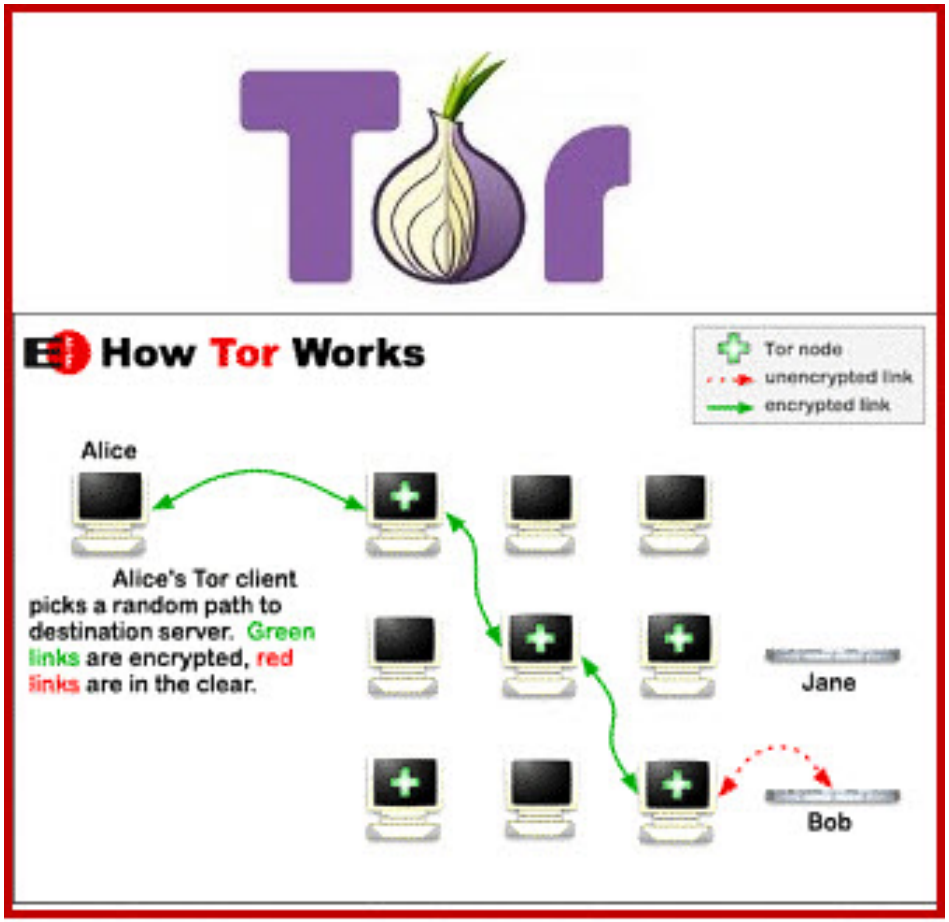
Outline

Outline

Tor

What is Tor ?

- The Tor network gives anonymity
- Its a type of low latency network
- Its the most commonly used service
- Comparatively easy to setup and use
- Require at-least 3 hops

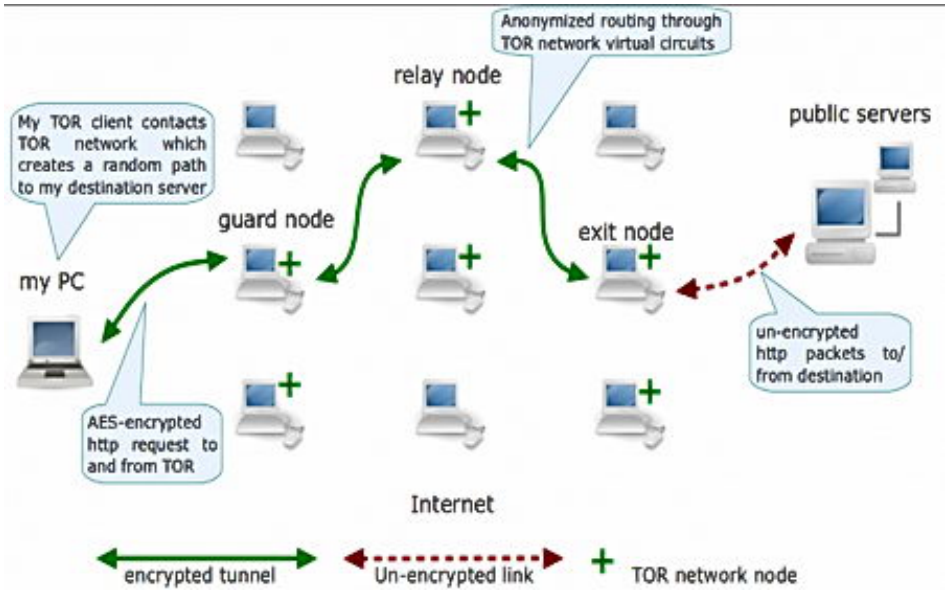


INDRAPRASTHA INSTITUTE of INFORMATION TECHNOLOGY DELHI

Tor Design

How does it work ?

- Over 6000+ routers called OR's
- Build a circuit and expose over socks proxy
- 10 min circuit idle time.
- Has A queuing architecture.
- Round robin for circuit scheduling.
- Randomly choose Routers.



Basic Tor Network[1]

Image Scraped from Internet

INDRAPRASTHA INSTITUTE of INFORMATION TECHNOLOGY DELHI

Outline

INDRAPRASTHA INSTITUTE of INFORMATION TECHNOLOGY DELHI

Design Weakness

What's wrong ?

- Tor is not scalable
- Some attacks are possible without full circuit control
- Transport design is an attack vector.
- No congestion control
- Expensive circuit creation time.

Outline

Classification of studies

What's new and old !

- Traffic Management
- Router Selection
- Scalability
- Circuit Construction

INDRAPRASTHA INSTITUTE of INFORMATION TECHNOLOGY DELHI

Outline

INDRAPRASTHA INSTITUTE of INFORMATION TECHNOLOGY DELHI

Traffic Management

Improving scheduling of traffic

- Incentive-based Schemes.
- Multi-path routing.
- Congestion Control.

Some important works:

- TCP over DTLS
- KIST
- UDP-OR
- uTOR

INDRAPRASTHA INSTITUTE of INFORMATION TECHNOLOGY DELHI

Outline

INDRAPRASTHA INSTITUTE of INFORMATION TECHNOLOGY DELHI

Router Selection

- Tuneable Selection
- Link-Based Selection
- LasTOR
- Congestion-aware Routing
- Comprehensive Evalauation.

Outline

INDRAPRASTHA INSTITUTE of INFORMATION TECHNOLOGY DELHI

Scalability

- Peer-to-Peer Approaches
- PIR-Tor

INDRAPRASTHA INSTITUTE of INFORMATION TECHNOLOGY DELHI

Outline

INDRAPRASTHA INSTITUTE of INFORMATION TECHNOLOGY DELHI

Circuit Construction

- Improved Diffie-Hellman Based Key Agreement.
- Pairing Based Onion Routing.
- Certificateless Onion Routing.

Outline

INDRAPRASTHA INSTITUTE of INFORMATION TECHNOLOGY DELHI

Attacks

- Passive Attacks
  - AS-Level Adversary
  - Website Fingerprinting
- Active Attacks
  - End to End Confirmation Attacks
  - Path Selection Attacks
  - Side Channel Attacks

Outline

INDRAPRASTHA INSTITUTE of INFORMATION TECHNOLOGY DELHI

Unresolved Issues

- Bot-nets
- Blocking Resistance
- Performance

Takeaways

- Identification of key weakness of TOR.
- Classification of research work.
- Survey in each of the category of research.

Questions

INDRAPRASTHA INSTITUTE of INFORMATION TECHNOLOGY DELHI

For Further Reading I


Tor Website.
www.torproject.org