Anonymizing Activities

Kevin Koo

(kevinkoo001@gmail.com)

개요

- Tor History
- Tor Concept
- AdvOR@Windows
- torsocks@Linux (Installation & Usage)
- Tor Pitfalls
- Privoxy
- Proxy Type
- Anonymizers & De-Anonymizers

Tor (The Onion Routing) History

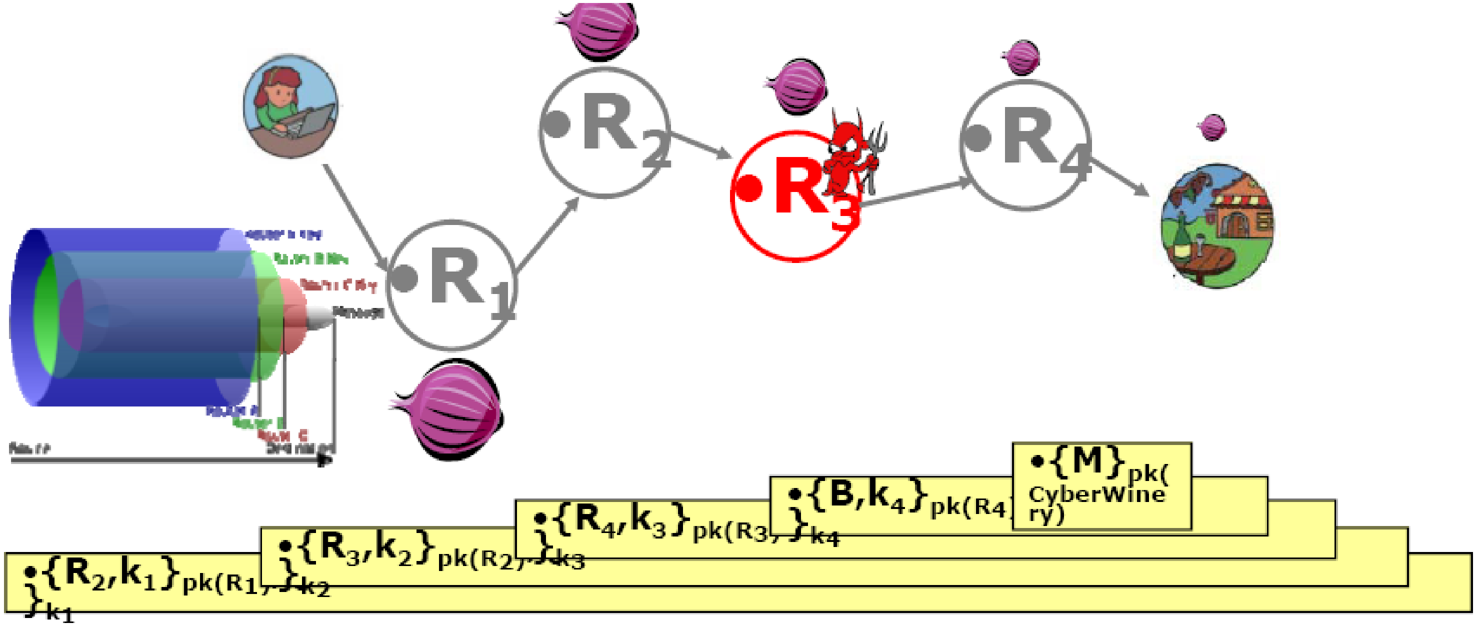
- History
  - Roger Dingledine, Nick Mathewson and Paul Syverson, “Tor: The Second-Generation Onion Router" at the 13th USENIX Security Symposium (08.13.2004)
  - Sponsored by the US Naval Research Laboratory
    Financially supported by the Electronic Frontier Foundation
  - Awarded the Free Software Foundation's 2010 Award for Projects of Social Benefit

http://www.torproject.org

http://sourceforge.net/projects/advtor/

Tor (The Onion Routing) Concept

- A network of virtual tunnels that allows people and groups to improve their privacy on the Internet.
- Routing information for each link encrypted with the public key.
- Each router learns only the identity of the next router



$\bullet\{R_2,k_1\}_{pk(R_1)}, \}_{k_1}$

$\bullet\{R_3,k_2\}_{pk(R_2)}, \}_{k_2}$

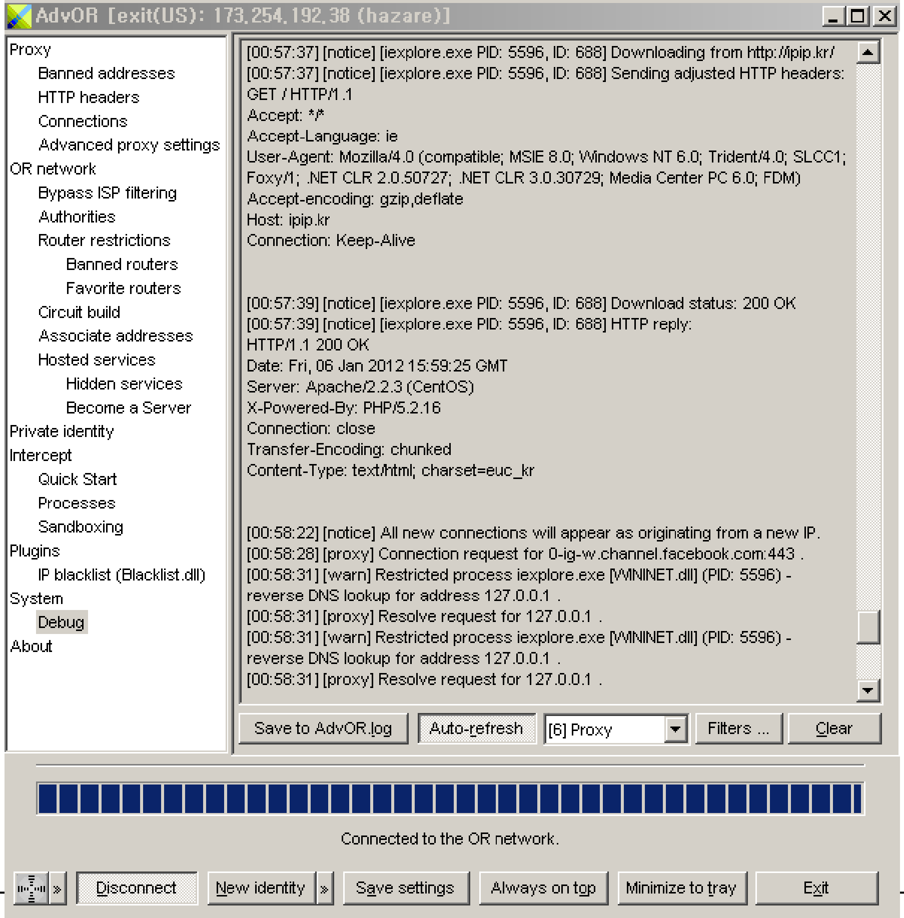
$\bullet\{R_4,k_3\}_{pk(R_3)}, \}_{k_3}$

$\bullet\{B,k_4\}_{pk(R_4)}, \}_{k_4}$

$\bullet\{M\}_{pk(CyberWinery)}$

AdvOR@Windows (Installation & Usage)

- Default Port: 9001
- Supports Socks4, Socks5, HTTP, HTTPS
  SOCKS4 VS SOCKS5 (supports Proxy Authentication)
- Specifies browse type, version, OS, extensions
- Restricts connections only from specific IPs or IP Ranges
- Selects
  Exit node
  New Identity
  Banned routers
  Favorite routers
  IP Blacklist



```
[00:57:37] [notice] [iexplore.exe PID: 5596, ID: 688] Downloading from http://ipip.kr/
[00:57:37] [notice] [iexplore.exe PID: 5596, ID: 688] Sending adjusted HTTP headers:
GET / HTTP/1.1
Accept: */*
Accept-Language: ie
User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.0; Trident/4.0; SLCC1;
Foxy/1; .NET CLR 2.0.50727; .NET CLR 3.0.30729; Media Center PC 6.0; FDM)
Accept-encoding: gzip,deflate
Host: ipip.kr
Connection: Keep-Alive


[00:57:39] [notice] [iexplore.exe PID: 5596, ID: 688] Download status: 200 OK
[00:57:39] [notice] [iexplore.exe PID: 5596, ID: 688] HTTP reply:
HTTP/1.1 200 OK
Date: Fri, 06 Jan 2012 15:59:25 GMT
Server: Apache/2.2.3 (CentOS)
X-Powered-By: PHP/5.2.16
Connection: close
Transfer-Encoding: chunked
Content-Type: text/html; charset=euc_kr


[00:58:22] [notice] All new connections will appear as originating from a new IP.
[00:58:28] [proxy] Connection request for 0-ig-w.channel.facebook.com:443 .
[00:58:31] [warn] Restricted process iexplore.exe [WININET.dll] (PID: 5596) -
reverse DNS lookup for address 127.0.0.1 .
[00:58:31] [proxy] Resolve request for 127.0.0.1 .
[00:58:31] [warn] Restricted process iexplore.exe [WININET.dll] (PID: 5596) -
reverse DNS lookup for address 127.0.0.1 .
[00:58:31] [proxy] Resolve request for 127.0.0.1 .
```

torsocks@Linux (Installation & Usage)

Default Port: 9050

```
# apt-get install –y torsocks
# wget http://ipip.kr
# usewithtor wget http://ipip.kr
# usewithtor wget http://ipip.kr -U "Mozilla/5.0 (Windows NT;
   en-US) Gecko/20100316 firefox/3.6.2”
# usewithtor ssh id@myweb.hosting.com
# ./tgrab.sh http://ipip.kr
```

torsocks@Linux (Installation & Usage)

- SocksiPy.zip
  (http://socksipy.sourceforge.net, http://sourceforge.net/projects/socksipy)

```
# cp socks.py /usr/lib/python2.7/dist-package
```

- torwget.py
  : SOCKS proxy initialization, socket object → SocksiPy class overriding)
  : socks.setdefaultproxy(proxy((socks.proxy (PROXY_TYPE_SOCKS5,
  TOR_SERVER, TOR_PORT)
  socket.socket = socks.socksocket
  : TOR_SERVER = “127.0.0.1”, TOR_PORT=9050

- http://malc0de.com/database/
- xnxxvideos.xn.funpic.org/dll.exe (2012.1.1)

```
# python torwget.py -c xnxxvideos.xn.funpic.org/dll.exe -r http://msn.com –z

xnxxvideos.xn.funpic.org/dll.exe Hostname: xnxxvideos.xn.funpic.org
Path: /dll.exe
Headers: {'Referrer': 'http://msn.com', 'Accept': '*/*', 'User-Agent': 'Opera/9.51 (Macintosh; Intel Mac
OS X; U; en)'}
Saving 786432 bytes to xnxxvideos. xn.funpic.org/dll.exe
Done!
```

Tor Pitfalls

- Speed
- Untrusted tor user (Exit node)
- Tor block list

Privoxy

- Port 8118
- Feasibility
  filter banner ads, web bugs, and HTML annoyances
  bypass click-tracking scripts and redirections
  remove animation from GIFs

```
# apt-get install privoxy

# netstat –anlpt
  Active Internet connections (servers and established)
  Proto Recv-Q Send-Q Local Address     Foreign Address   State PID/Program name
  tcp        0      0 127.0.0.1:8118          0.0.0.0:*               LISTEN      10315/privoxy
```

- http://www.privoxy.org,
  http://sourceforge.net/projects/ijbswa/files/
- /etc/privoxy/config

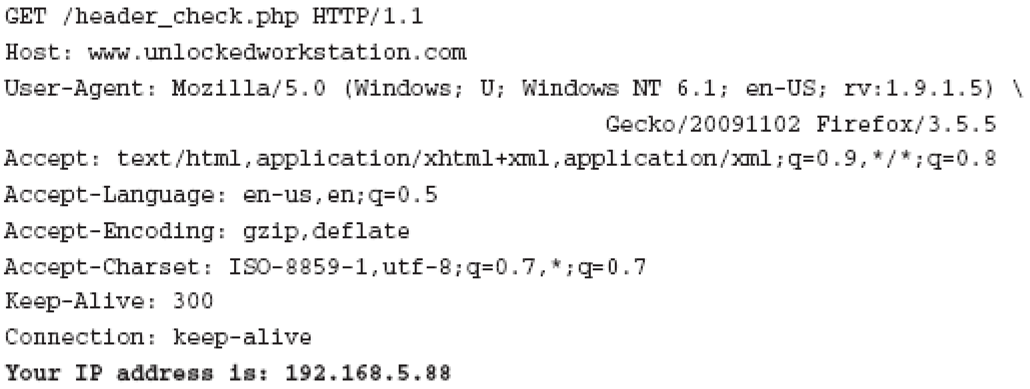
```
forward-socks5   /              127.0.0.1:9050 .
```

Proxy Type

- Transparent Proxy
- Anonymous Proxy
- Highly Aanonymous Proxy

header_check.php

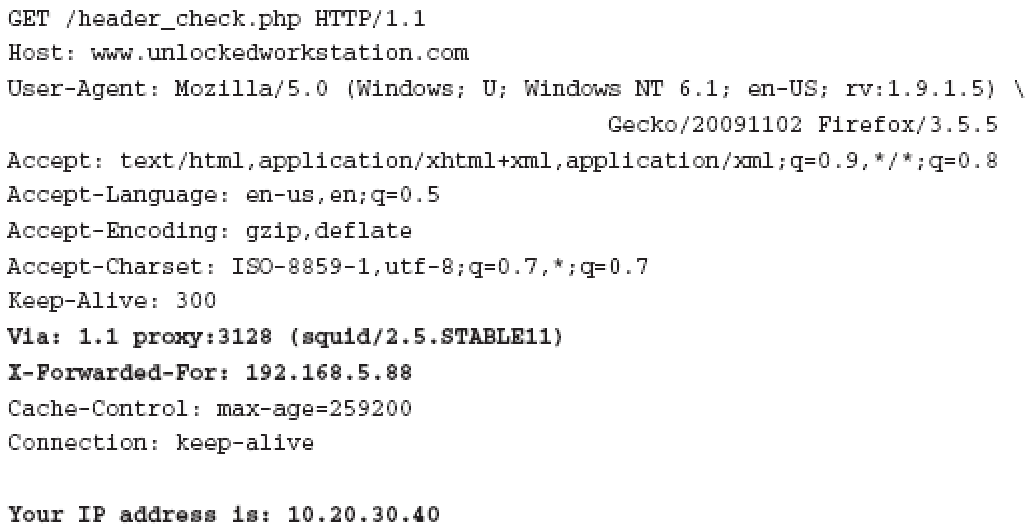
```
<?php
$get_headers = apache_request_headers();
echo $_SERVER['REQUEST_METHOD'] . " " .
$_SERVER['REQUEST_URI'] . " " .
$_SERVER['SERVER_PROTOCOL'] . "<br/>";
foreach ($get_headers as $header => $value) {
echo "$header: $value <br/>₩n";
}
echo "<br/><br/>Your IP address is: " . $_SERVER['REMOTE_ADDR'];
?>
```



```
GET /header_check.php HTTP/1.1
Host: www.unlockedworkstation.com
User-Agent: Mozilla/5.0 (Windows; U; Windows NT 6.1; en-US; rv:1.9.1.5) \
                                            Gecko/20091102 Firefox/3.5.5
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-us,en;q=0.5
Accept-Encoding: gzip,deflate
Accept-Charset: ISO-8859-1,utf-8;q=0.7,*;q=0.7
Keep-Alive: 300
Connection: keep-alive
Your IP address is: 192.168.5.88
```

Proxy Type: Transparent

- Transparent Proxy
  http://www.proxy4free.com/

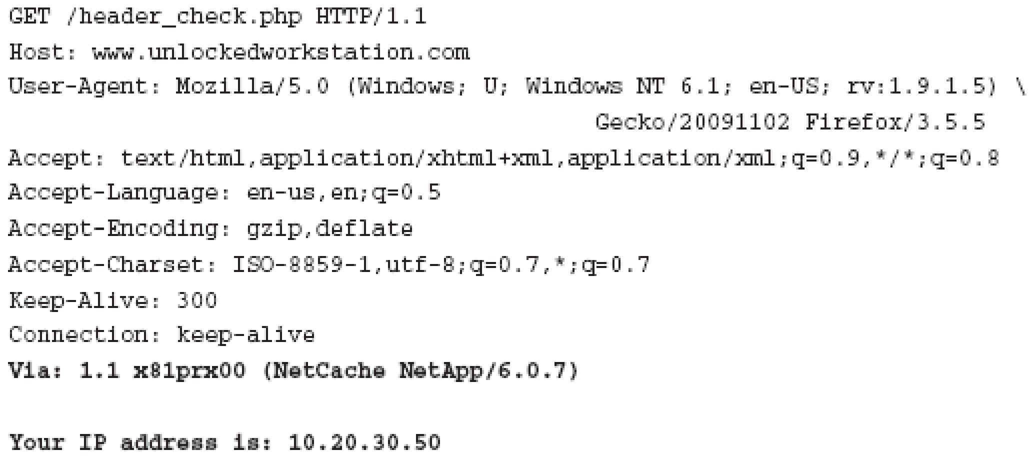


```
GET /header_check.php HTTP/1.1
Host: www.unlockedworkstation.com
User-Agent: Mozilla/5.0 (Windows; U; Windows NT 6.1; en-US; rv:1.9.1.5) \
                                           Gecko/20091102 Firefox/3.5.5
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-us,en;q=0.5
Accept-Encoding: gzip,deflate
Accept-Charset: ISO-8859-1,utf-8;q=0.7,*;q=0.7
Keep-Alive: 300
Via: 1.1 proxy:3128 (squid/2.5.STABLE11)
X-Forwarded-For: 192.168.5.88
Cache-Control: max-age=259200
Connection: keep-alive

Your IP address is: 10.20.30.40
```

Proxy Type: Anonymous

- Anonymous Proxy
  http://www.youhide.com/

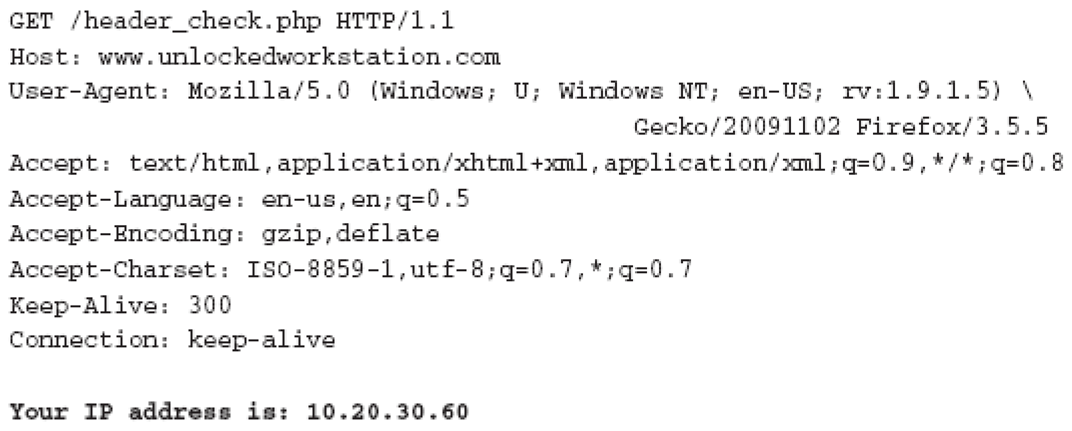


```
GET /header_check.php HTTP/1.1
Host: www.unlockedworkstation.com
User-Agent: Mozilla/5.0 (Windows; U; Windows NT 6.1; en-US; rv:1.9.1.5) \
                                          Gecko/20091102 Firefox/3.5.5
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-us,en;q=0.5
Accept-Encoding: gzip,deflate
Accept-Charset: ISO-8859-1,utf-8;q=0.7,*;q=0.7
Keep-Alive: 300
Connection: keep-alive
Via: 1.1 x81prx00 (NetCache NetApp/6.0.7)

Your IP address is: 10.20.30.50
```

Proxy Type: Highly Anonymous

- Highly Anonymous Proxy
  http://aliveproxy.com/high-anonymity-proxy-list/



```
GET /header_check.php HTTP/1.1
Host: www.unlockedworkstation.com
User-Agent: Mozilla/5.0 (Windows; U; Windows NT; en-US; rv:1.9.1.5) \
                                          Gecko/20091102 Firefox/3.5.5
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-us,en;q=0.5
Accept-Encoding: gzip,deflate
Accept-Charset: ISO-8859-1,utf-8;q=0.7,*;q=0.7
Keep-Alive: 300
Connection: keep-alive

Your IP address is: 10.20.30.60
```

Anonymizers & De-Anonymizers

- Web Anonymizer
  http://www.anonymouse.org

- Cellular Internet Connections

- http://panopticlick.eff.org/
  This site tests your browser to see how unique it is based on the information it will share with sites it visits. (http://panopticlick.eff.org/browser-uniqueness.pdf)

  Panopticlick
  How Unique — and Trackable — Is Your Browser?

- http://browserspy.dk/
  This site shows you just how much information can be retrieved from your browser just by visiting a page.

  BrowserSPY.dk