LIRA: Lightweight Incentivized Routing for Anonymity

20th Annual Network & Distributed System Security Symposium
February 27, 2013

Rob Jansen
Aaron Johnson
Paul Syverson
U.S. Naval Research Laboratory
Problem
Onion Routing

User

Onion Routers

Destination

encrypted

unencrypted
Onion Routing

User

Onion Routers

encrypted

unencrypted

Destination
Onion Routing

User

Onion Routers

encrypted

unencrypted

Destination
Onion Routing

User -> Onion Routers (encrypted) -> Destination

Onion Routers

torproject.org
Onion Routing

User

Onion Routers

encrypted

unencrypted

Destination

torproject.org
Tor is Slow

Web (320 KiB)  
Bulk (5 MiB)

Cumulative Fraction

Time to Last Byte (s)

plab  
tor
Tor Utilization

~3000 relays
Tor Utilization

~500,000 users/day

~3000 relays
Tor Utilization

Total relay bandwidth

- Advertised bandwidth
- Bandwidth history

The Tor Project – https://metrics.torproject.org/
# Tor’s Top 20 Exit Relays

<table>
<thead>
<tr>
<th>Exit Probability</th>
<th>Advertised Bandwidth</th>
<th>Nickname</th>
<th>Country</th>
</tr>
</thead>
<tbody>
<tr>
<td>7.25%</td>
<td>0.87%</td>
<td>chaoscomputerclub18</td>
<td>DE</td>
</tr>
<tr>
<td>6.35%</td>
<td>0.93%</td>
<td>chaoscomputerclub20</td>
<td>DE</td>
</tr>
<tr>
<td>5.92%</td>
<td>1.48%</td>
<td>herngaard</td>
<td>US</td>
</tr>
<tr>
<td>3.60%</td>
<td>0.66%</td>
<td>chomsky</td>
<td>NL</td>
</tr>
<tr>
<td>3.35%</td>
<td>1.17%</td>
<td>dorrisdeebrown</td>
<td>DE</td>
</tr>
<tr>
<td>3.32%</td>
<td>1.18%</td>
<td>bolobolo1</td>
<td>DE</td>
</tr>
<tr>
<td>3.26%</td>
<td>0.65%</td>
<td>rainbowwarrior</td>
<td>NL</td>
</tr>
<tr>
<td>2.32%</td>
<td>0.36%</td>
<td>sdnettor01</td>
<td>SE</td>
</tr>
<tr>
<td>2.23%</td>
<td>0.69%</td>
<td>TheSignul</td>
<td>RO</td>
</tr>
<tr>
<td>2.22%</td>
<td>0.41%</td>
<td>raskin</td>
<td>DE</td>
</tr>
<tr>
<td>2.05%</td>
<td>0.40%</td>
<td>bouazizi</td>
<td>DE</td>
</tr>
<tr>
<td>1.93%</td>
<td>0.65%</td>
<td>assk</td>
<td>SE</td>
</tr>
<tr>
<td>1.82%</td>
<td>0.39%</td>
<td>kramse</td>
<td>DK</td>
</tr>
<tr>
<td>1.67%</td>
<td>0.35%</td>
<td>BostonUCompSci</td>
<td>US</td>
</tr>
<tr>
<td>1.53%</td>
<td>0.40%</td>
<td>bach</td>
<td>DE</td>
</tr>
<tr>
<td>1.31%</td>
<td>0.73%</td>
<td>DFRI0</td>
<td>SE</td>
</tr>
<tr>
<td>1.26%</td>
<td>0.31%</td>
<td>Amunet2</td>
<td>US</td>
</tr>
<tr>
<td>1.13%</td>
<td>0.27%</td>
<td>Amunet8</td>
<td>US</td>
</tr>
<tr>
<td>0.84%</td>
<td>0.27%</td>
<td>chaoscomputerclub28</td>
<td>DE</td>
</tr>
<tr>
<td>0.76%</td>
<td>0.37%</td>
<td>DFRI3</td>
<td>SE</td>
</tr>
</tbody>
</table>

Total: 54.14%
2008*

Bytes

- BitTorrent: 40%
- HTTP: 58%

2010**

Flows

- BitTorrent: 3%
- HTTP: 92%

- Other: 11%

- Other: 69%

*McCoy et al. PETS 2008, **Chaabane et al. NSS 2010
Our Solution
Incentive Scheme

- LIRA

Relays’ own traffic gets better performance
Incentive Schemes

- LIRA
- Gold star
- Tortoise
- BRAIDS
- Freedom
- PAR
- XPay

Relays’ own traffic gets better performance
Charge users, pay relays
## Incentive Schemes

<table>
<thead>
<tr>
<th></th>
<th>External payment</th>
<th>Non-relays pay</th>
<th>Efficiency concerns</th>
<th>Anonymity concerns</th>
</tr>
</thead>
<tbody>
<tr>
<td>Freedom</td>
<td>✗</td>
<td>✗</td>
<td></td>
<td></td>
</tr>
<tr>
<td>PAR</td>
<td>✗</td>
<td>✗</td>
<td></td>
<td></td>
</tr>
<tr>
<td>XPay</td>
<td>✗</td>
<td>✗</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Gold star</td>
<td></td>
<td></td>
<td></td>
<td>✗</td>
</tr>
<tr>
<td>Tortoise</td>
<td></td>
<td></td>
<td></td>
<td>✗</td>
</tr>
<tr>
<td>BRAIDS</td>
<td></td>
<td></td>
<td></td>
<td>✗</td>
</tr>
</tbody>
</table>
Anonymous Incentives

Problem: Priority identifies user as a relay
Anonymous Incentives

Problem: Priority identifies user as a relay

Solutions

1. Give some priority “tickets” to all users (BRAIDS).
Anonymous Incentives

Problem: Priority identifies user as a relay

Solutions
1. Give some priority “tickets” to all users (BRAIDS).
2. Cryptographic lottery gives priority; winning tickets can be (secretly) bought (LIRA).
LIRA Design

Bank
LIRA Design

Bank gives anonymous coins to relays based on amount of traffic forwarded
LIRA Design

Bank sets up lottery with each relay
LIRA Design

Buy “winners” with coins
LIRA Design

Clients guess winners
Cryptographic Lotteries

- Lottery at relay $r$
  \[ g_r: \{0,1\}^{2L} \rightarrow \{0,1\}^{2L} \]
  x wins if
  - $g_r(x) = y_0 \ || \ y_1$
  - $0 \leq y_0 \oplus y_1 < p \ 2^L$
Cryptographic Lotteries

- Lottery at relay $r$
  $g_r: \{0,1\}^{2L} \rightarrow \{0,1\}^{2L}$
  $x$ wins if
  - $g_r(x) = y_0 \parallel y_1$
  - $0 \leq y_0 \oplus y_1 < p \cdot 2^L$

- $g_r$ defined from PRF $f_r$ using a Luby-Rackoff-like construction
  - $y_0 = f_r(x_1) \oplus x_0$
  - $y_1 = f_r(y_0) \oplus x_1$
  - $g_r(x) = y_0 \parallel y_1$
Cryptographic Lotteries

• Lottery at relay \( r \)
  \( g_r \colon \{0,1\}^{2L} \rightarrow \{0,1\}^{2L} \)
x wins if
  – \( g_r(x) = y_0 \parallel y_1 \)
  – \( 0 \leq y_0 \oplus y_1 < p \cdot 2^L \)

• \( g_r \) defined from PRF \( f_r \) using a Luby-Rackoff-like construction
  – \( y_0 = f_r(x_1) \oplus x_0 \)
  – \( y_1 = f_r(y_0) \oplus x_1 \)
  – \( g_r(x) = y_0 \parallel y_1 \)

• \( f_r(x) = H(H(H(x) x_r d))) \)
  – \( H \) is a hash function
  – \( x_r \) is public; bank gives \( x_r d \) to \( r \) during setup,
  – \( d \) is bank’s private RSA key
Analysis
### Efficiency

<table>
<thead>
<tr>
<th></th>
<th>LIRA</th>
<th>BRAIDS</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Bank</strong></td>
<td>Blind signatures/s</td>
<td>127.5+127.5f (256B/sig)</td>
</tr>
<tr>
<td><strong>Relay</strong></td>
<td>Priority verification</td>
<td>6 hashes (18 us)</td>
</tr>
<tr>
<td><strong>Normal Client</strong></td>
<td>Tickets / connection</td>
<td>0</td>
</tr>
</tbody>
</table>

$f$ is fraction of credit redeemed.

Entire network is transferring 1700 MiB/s.
Signature size: 1024 bits. Ticket size: 320 bits.
Linux OpenSSL benchmarks on Intel Core2 Duo 2.67 GHz
Anonymity

• With m buyers and n guessers, the probability that a prioritized circuit source is a given buyer is

$$\frac{1}{m + np^3}$$

compared to $1/(m+n)$ without priority.

• Linked priority degrades anonymity exponentially to $1/m$. 
Performance

Web (320 KiB)  Bulk (5 MiB)
Performance, More Capacity

Web (320 KiB)  Bulk (5 MiB)
Conclusion

1. Volunteer-run Tor network is overloaded.
2. LIRA provides incentives to contribute by rewards with better network performance.
3. LIRA is more efficient than previous schemes while maintaining anonymity.
4. Full-network experiments demonstrate better performance and scalability.
Buying winning tickets

- Client chooses \(y_0, y_1, 0 \leq y_0 \text{ XOR } y_1 < p2^L\)
- Using PRF protocol, client reverses Luby-Rackoff process to get \(g_r^{-1}(y_0 \parallel y_1)\).

Client \(c\) and bank \(B\) evaluate \(f_r(x)\)
1. \(C\) sends \(a^e x^d_r\) to \(B\), \(a\) random.
2. \(B\) returns \(abx^d_r\), \(b\) random.
3. \(c\) sends \(b \text{ H}(x)x^d_r\) to \(B\).
4. \(B\) returns \(\text{H}(\text{H}(x)x^d_r)\) to \(c\).
5. \(c\) outputs \(f_r(x) = \text{H}(x \text{ H}(\text{H}(x)x^d_r)))\).

PRF Protocol
Winning circuits are prioritized

1. Client sends tickets to each relay in circuit.
2. Relays evaluate tickets. Winners must have unseen PRF inputs. Neighbors sent results.
3. If ticket wins and neighbors report wins, circuit is prioritized for next $\beta$ bytes.
Priority Scheduling

• Proportional Differentiated Services
  – Split traffic into “paid” and “unpaid” classes
  – Prioritize classes using quality differentiation parameters $p_i$ and quality measure $Q$ (EWMA)

$$\frac{p_1}{p_2} = \frac{Q_1(\Delta t)}{Q_2(\Delta t)}$$
Bank secrecy (honest-but-curious)

- Clients oblivious to $x_r^d$.
- B cannot produce $r$, input $x$, or output $f_r(x)$.
- Relay purchases are batched, preventing bank from knowing when prioritized circuits are constructed.

\[
\begin{align*}
&c \text{ and } B \text{ evaluate } f_r(x) \\
1. & \quad c \text{ obtains } b x_r^d. \\
2. & \quad c \text{ sends } b \ H(x)x_r^d \text{ to } B. \\
3. & \quad B \text{ sends } H(H(x)x_r^d) \text{ to } c. \\
4. & \quad c \text{ outputs } H(x(H(H(x)x_r^d))).
\end{align*}
\]
Creating winning tickets

- \( f_r \) is random in ROM when \( x_r^d \) unknown.
- \( y_0 \) XOR \( y_1 \) is random. for \( y_0 \) or \( y_1 \) unknown
- One-time-use inputs to \( f_r \) prevent double spending.
- Tickets not fully purchased win with probability \( p \).

\[
f_r(x) = H(x(H(H(x) \cdot x_r^d))))
\]

\[
y_0 = f_r(x_1) \oplus x_0 \\
y_1 = f_r(y_0) \oplus x_1
\]

\[
g_r(x) = y_0 || y_1
\]

\[
0 \leq y_0 \oplus y_1 < p \cdot 2^L
\]

Cryptographic Lottery