Inferring Obfuscated Values in Freenet

Stefanie Roos, Florian Platzer, Jan-Michael Heller, Thorsten Strufe

TU Darmstadt, TU Dresden
Censorship-Resistance

- censorship-resistance needs anonymity
  - prevent attack or persecution of publishers

⇒ anonymisation services
  - federalised appr.
  - distributed appr.

- get rid of central trust entities

- protect freedom of speech
  - mandatory for democratic society
Anonymous Network Services 1/2

eg. login or request page

Application Layer

Software Layer

Network Layer

Jan-Michael Heller - FB 20 Informatik - TU Darmstadt - email: j_heller@rbg.informatik.tu-darmstadt.de
Anonymous Network Services 2/2

retrieve

Application Layer

store

Software Layer

Network Layer

Jan-Michael Heller - FB 20 Informatik - TU Darmstadt - email: j_heller@rbg.informatik.tu-darmstadt.de
Friend-to-Friend (f2f) networks

- nodes' connection based on users' real-life trust
- overlay built using given links
  - comparably low number of links
  - no additional connections can be established to increase efficiency
- tradeoff: anonymity vs. performance

Jan-Michael Heller - FB 20 Informatik - TU Darmstadt - email: j_heller@rbg.informatik.tu-darmstadt.de
Freenet

- Goal: allow censorship-resistant, anonymous content storage and retrieval
- data stored across peers (encrypted)
- combines opennet and f2f networks

bridge node (in both networks)
Probe Requests 1/2

• getting statistical information, esp. of friend-to-friend parts of the network
  – important: further development, attack analysis...
• ask peers for status and configuration values
  – random walk (with Metropolis-Hastings correction)
  – obfuscate numerical values
Probe Requests 2/2

- probe contains HTL counter
  - last decrement is omitted probabilistically
- on response each value is multiplicated by normally distrib. random value \((\mu = 1, \sigma \text{ value specific})\)
- idea: do not allow identification, but keep global statistics intact
Probe Requests 2/2

• probe contains HTL counter
  - last decrement is omitted probabilistically

• on response each value is multiplicated by normally distributed random value (μ = 1, σ specific)

• idea: do not allow identification, but keep global statistics intact

Attack idea:
  • identify bridge nodes using probe information
  • find f2f networks
Attack sketch

- Send $m$ probes with max. HTL into network
  - calculate overall distribution
- connect to a target node to infer hidden value
- send $n$ probe requests with HTL = 1 to desired node
- use bayesian learning model on answers
- choose most likely value in posterior as inferred value
Evaluation

- **goal**
  - find discrepancy in number of possible neighbours given by guessed value and actually connected neighbours

- **simulation**
  - need to evaluate attack, but no ground truth for real world network, connection to nodes slow
  - construction of test network costly

- **real client experiment**
  - check if simulation results fit attack on real clients
Simulation Experiment

• construct a sample network
  – comparable to Freenet topology
  – 5,000 nodes
  – assign bandwidths gathered from real world Freenet statistic

• obtain global statistic inside simulation by sending 10,000 probe requests

• infer bandwidth of 50 random nodes based on 2,000 probe samples
**Simulation Results 2/2**

- **real world experiment**
  - insert 2 nodes into Freenet network
    - one as attacker and one as victim
  - send probes from attacking node to victim
  - infer value, compare to actually set value

<table>
<thead>
<tr>
<th>x</th>
<th>Error</th>
<th>Certainty (TP)</th>
<th>Certainty (FP)</th>
<th>Certainty (FN)</th>
</tr>
</thead>
<tbody>
<tr>
<td>16</td>
<td>0:10</td>
<td>1.0 [1.0,1.0]</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>64</td>
<td>0:10</td>
<td>0.998 [0.992,1]</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>85</td>
<td>0:8, 1:2</td>
<td>0.846 [0.518,1]</td>
<td>0.902 [0.901,0.903]</td>
<td>0.098 [0.097,0.099]</td>
</tr>
<tr>
<td>2000</td>
<td>0:10</td>
<td>1.0 [1.0,1.0]</td>
<td>-</td>
<td>-</td>
</tr>
</tbody>
</table>
Fixing the Probe Obfuscation

• use \( k-1 \) static shadow values based on a global distribution \( H \) instead of really forwarding
  – \( k \)-anonymous statistics
• on probe request with HTL = 1, return either obfuscated local value or obfuscated shadow value
• problems
  – how to get global distribution
  – when to change shadow values
Conclusion

• showed that Freenet stats are not anonymous
• thus sensible network structure information could be revealed
• evaluation in simulation and real world experiment
• fix developed and is being integrated into network