Social attacks against anonymity networks

Nick Mathewson
The Tor Project
<nickm@torproject.org>

Defcon XV
Aug 4, 2007
That title was confusing!

- What I mean by “social attacks.”
- What I mean by “anonymity network.”

Not covered here

- How to be a more effective social engineer.
Outline

• Intro to anonymity networks.
  – Basics of traffic analysis
  – Why use social engineering?
• Trivial attacks: no traffic analysis required.
• Attacks to help traffic analysis.
  – Traffic gathering: more input for your attack.
  – Network partitioning: better input for your attack.
• Defenses
Basic idea: anonymity networks hide users among users...
...but when users act differently, an observer can tell them apart.
...and separating users keeps them from blending.
We use distributed networks so no one server can compromise users' traffic

Ex.: Tor, Remailers, Mixminion...
Against low-latency networks: watch both ends and correlate traffic.

If patterns (approximately) match, Alice1 is talking to Bob2.
Against high-latency networks: compare net with Alice to net without.

ex: cpunk, MixMaster, Mixminion

<table>
<thead>
<tr>
<th></th>
<th>Bob1</th>
<th>Bob2</th>
<th>Bob3</th>
<th>Bob4</th>
</tr>
</thead>
<tbody>
<tr>
<td>Alice Sending</td>
<td>10</td>
<td>13</td>
<td>8</td>
<td>2</td>
</tr>
<tr>
<td>Alice not sending</td>
<td>9</td>
<td>13</td>
<td>8</td>
<td>1</td>
</tr>
</tbody>
</table>

This ("long-term intersection") attack needs lots of traffic.

So why not always use high-latency nets? Too slow.
So, what should a smart attacker do?

- If possible, try to remove benefits of network from user.
- Otherwise, try to speed up traffic analysis.
  - Get more traffic.
  - Make the traffic you get more useful.
  - Lower volume of background traffic (High-latency nets only.)
Never attribute to malice...

- Caveat 1: Many harmful ideas occur to people spontaneously.

- Caveat 2: Many harmful ideas are true.
I. Trivial attacks

Or,
“We’re jumping off a cliff. Wanna come?”
Why attack the network when you can circumvent it?

- “To view my flash site, just enable plugins.” *
- “Click here for skype.” *
- “I’m not getting your mail. Just use yahoo, okay?” *
- “I love your ideas, and would like to donate.”
- “I love your ideas, and would like to meet.” *
Why attack the network when you can replace it?

- “Your traffic will be even more secure with anon2000!”*
- “I just read an attack paper on VSN. We should all use ObscureNet!” *
- “VSN has a seekrit backdoor!” *
"Help me with my criminal investigation of Alice, or else." *
  ● ("Why of course I’m an FBI agent! Would I lie?") *
● "Say, we’re looking for a bug. Send me your logs?"
● "Here’s some extra-fast extra-stable server software!" *
Long-term: make the network unmaintained.

Can you make developers and providers quit?

- “Developer X is a jerk!” *
- “Dear Developer X. Thank you for the fine software. I enjoy using it for my nasty cause!” *
- “I am a provider, and I am quitting out of fear!” *
II. Getting more traffic

Or,
“traffic analysis is easy for the popular kids”
The more traffic you see, the more users you compromise...
So try to make your service popular!
How to win traffic and compromise people

• “Please use my excellent server.” *
• “I’ve added extra features to my server.” *
• “Guide to better performance: Use fast servers. Like mine.” *
• “Don’t use Bob’s server...
  • it’s compromised.” *
  • it’s surveiled.” *
  • it’s in a bad country!” *
III. Partitioning attacks

Or,
“you can’t tell whether it was me, myself, or I!”
Network partitioning 1: split one big network into many small networks.
Network partitioning 1: split one big network into many small networks.
Partitioning 2: When users like different servers, they provide less cover for each other.
It's easier to get a large foothold in a small subset of servers...
When users know servers at random, you can partition them into tiny sets.

Only \((.4)(.2)(.8) = .064\) of users will use this sequence in their paths.
How to encourage partitioning.

• “Here is my list of extra-good servers.” *
  • “Here’s mine...”
• “Don’t use any servers in Germany or France.” *
  • “No, don’t use any in the USA!”
    • “Don’t use Germany or USA. France is fine...”
  • ...
• Start operator feuds.
• “Hi, I’m an operator, and I’m evil.” *
  • “I agree with evil operator!” “I don’t!”
  • ...

* *= Additional information or context
User preferences are a great partitioning opportunity. *
If you can't partition the network, you can try partitioning the traffic.

“Needless options are bad for you.”
IV. Defenses
Consensus-based server selection stops lots of network partitioning.

- Provide a good default list of servers, and make it easy to use.
  (Needs to be self-updating and secure.)

- Example: Tor vs cpunk
Is this trioption really necessary?

- Bad options: ciphersuite, padding len...
  - cf. “painting the bikeshed”

- Good options:
Providers need thick skins.

• People will tell you stuff to get you to stop being a provider.
  • True stuff?
  • In perspective?

• People will try to start provider flamewars.
Demand clear descriptions of attacks.

• Is this attack novel?
  • (Hint: RTFFFAQ.)

• What are the requirements/results?

• Is this attack any better than end-to-end correlation?

• Does this attack work against other systems of this kind?
Paranoia is for newbs: Be meta-paranoid.

- Paranoia: Trust nobody completely.

- Meta-Paranoia: This includes the people telling you not to trust people.
Follow information to its source.

I’m suspicious of “some guy”: he likes to spread really awful information.
Shameless plugs

• Tor: [https://torproject.org](https://torproject.org)
  – Try it out; want to run a server?
  – See docs and specs for more detail.

• Donate to Tor!
  – [https://torproject.org/donate.html](https://torproject.org/donate.html)
  – (We’re a tax-deductible charity!)

• Donate to EFF too!
  – I’m in the dunk tank at 6:30

• See more talks!
  – Roger at 2 on anti-censorship
  – Mike at 5 on securing the network and apps.