Online Anonymity & Privacy

Andrew Lewman
The Tor Project
https://torproject.org/
Outline

- Why anonymity?
- Crash course on Tor
- Future
Informally: anonymity means you can't tell who did what

“Who wrote this blog post?”

“Who's been viewing my webpages?”

“Who's been emailing patent attorneys?”
Formally: anonymity means indistinguishability within an “anonymity set”.

Attacker can't tell which Alice is talking to Bob!
Anonymity isn't cryptography: Cryptography just protects contents.

Alice

“Hi, Bob!”

<gibberish>

attacker

“Hi, Bob!”

Bob
Anonymity isn't steganography: Attacker can tell that Alice is talking; just not to whom.

(Strong high-bandwidth steganography may not exist.)
Anonymity isn't just wishful thinking...

“You can't prove it was me!”

“Promise you won't look!”

“Promise you won't remember!”

“Promise you won't tell!”

“I didn't write my name on it!”

“Isn't the Internet already anonymous?”
...since “weak” anonymity isn't.

“You can't prove it was me!”

Proof is a very strong word. With statistics, suspicion becomes certainty.

Promise you won't look!”

Promise you won't remember!”

Promise you won't tell!”

Will others parties have the ability and incentives to keep their promises?

“I didn't write my name on it!”

Not what we're talking about.

“I didn't write my name on it!”

Not what we're talking about.

Nope!

(More info later.)

“Isn't the Internet already anonymous?”
Anonymity serves different interests for different user groups.

“It's privacy!”
Regular citizens don't want to be watched and tracked.

Hostile Bob

"I sell the logs."

Indifferent Bob

"Oops, I lost the logs."

Incompetent Bob

"Hey, they aren't my secrets."

Blogger Alice

8-year-old Alice

Sick Alice

Consumer Alice

Oppressed Alice

Name, address, age, friends, interests (medical, financial, etc), unpopular opinions, illegal opinions....

(the network can track too)
Anonymity serves different interests for different user groups.

- **Private citizens**: “It's privacy!”
- **Businesses**: “It's network security!”

Anonymity is illustrated as a concept connecting both user groups.
Businesses need to keep trade secrets.

“Oh, your employees are reading our patents/jobs page/product sheets?”

“Hey, it's Alice! Give her the 'Alice' version!”

“Wanna buy a list of Alice's suppliers? What about her customers? What about her engineering department's favorite search terms?”
Anonymity serves different interests for different user groups.

- Governments: “It's traffic-analysis resistance!”
- Businesses: “It's network security!”
- Private citizens: “It's privacy!”
Law enforcement needs anonymity to get the job done.

Officer Alice

- Investigated suspect
- Sting target
- Organized Crime

Witness/informer Alice

- Anonymous tips

"Why is alice.localpolice.gov reading my website?"

"Why no, alice.localpolice.gov! I would never sell counterfeits on ebay!"

"Is my family safe if I go after these guys?"

"Are they really going to ensure my anonymity?"
Governments need anonymity for their security

“What will you bid for a list of Baghdad IP addresses that get email from .gov?”

“What does the CIA Google for?”

“Do I really want to reveal my internal network topology?”

“What about insiders?”
Anonymity serves different interests for different user groups.

- **Governments**: "It's traffic-analysis resistance!"
- **Private citizens**: "It's privacy!"
- **Blocked users**: "It's reachability!"
- **Businesses**: "It's network security!"
You can't get anonymity on your own: private solutions are ineffective...

"One of the 25 users on AliceNet."

"Looks like a cop."

"It's somebody at AliceCorp!"
... so, anonymity loves company!
Current situation: Bad people on the Internet are doing fine

- Trojans
- Viruses
- Exploits
- Botnets
- Zombies
- Espionage
- DDoS
- Extortion
- Spam
- Phishing
IP addresses can be enough to bootstrap knowledge of identity.

- Alice 18.244.x.x
  - Hotlinked ad
  - Amazon account
  - Wikipedia post
Outline

- Why anonymity?
- Crash course on Tor
- Future
What is Tor?

- online anonymity software and network
- open source, freely available
- active research environment
The Tor Project, Inc.

- 501(c)(3) non-profit organization dedicated to the research and development of tools for online anonymity and privacy
Estimated 300,000 daily Tor users
The simplest designs use a single relay to hide connections.

(example: some commercial proxy providers)
But a single relay is a single point of failure.

Eavesdropping the relay works too.
So, add multiple relays so that no single one can betray Alice.
A corrupt first hop can tell that Alice is talking, but not to whom.
A corrupt final hop can tell that somebody is talking to Bob, but not who.
Alice makes a session key with R1

...And then tunnels to R2...and to R3
Who uses Tor?

- Normal people
- Law Enforcement
- Human Rights Activists
- Business Execs
- Militaries
- Abuse Victims
- https://torproject.org/torusers
• Tor doesn't magically encrypt the Internet
• Operating Systems and Applications leak your info
• Browser Plugins, Cookies, Extensions, Shockwave/Flash, Java, Quicktime, and PDF all conspire against you
Outline

• Why anonymity?
• Crash course on Tor
• Examples
Example 1: Pbd.ca
Example 2: cbc.ca
Advertising Network Reach

Combined Google Trackers
Percentage of domains in data set with at least one Google web bug
(393,829 unique domains in set)

- Google AdSense (1,393,873) - 35.5%
- Google Analytics (380,023) - 71.2%
- DoubleClick (104,935) - 26.5%
- Google FriendConnect (2,416) - 0.6%
- Google Widgets (2,457) - 0.6%

88.4%

(348,059)

Source: http://www.knowprivacy.org/
IP Address Only?

Whois record for 71.174.247.46 - Mozilla Firefox

IP Information for 71.174.247.46

IP Location: United States Dedham Verizon Internet Services Inc.
Resolve Host: pool-71.174-247-46.bstma.fios.verizon.net
IP Address: 71.174.247.46
Blacklist Status: Clear

OrgName: Verizon Internet Services Inc.
OrgID: VRIS
Address: 1880 Campus Commons Dr
City: Reston
StateProv: VA
PostalCode: 20191
Country: US

NetRange: 71.173.96.0 - 71.180.255.255
CIDR: 71.173.96.0/19, 71.173.128.0/17, 71.174.0.0/15, 71.176.0.0/14, 71.180.0.0/16
NetName: VIS-BLOCK
NetHandle: NET-71-173-96-0-1
Parent: NET-71-0-0-0-0
NetType: Direct Allocation
NameServer: NS1.VERIZON.NET
NameServer: NS2.VERIZON.NET
NameServer: NS3.VERIZON.NET
NameServer: NS4.VERIZON.NET
NameServer: NS5.VERIZON.NET
NameServer: NS6.VERIZON.NET
Comment: 
RegDate: 2005-06-01
Updated: 2009-10-14

OrgAbuseHandle: VISAB-ARIN
OrgAbuseName: VIS Abuse
OrgAbusePhone: +1-214-513-6711
OrgAbuseEmail: security@verizon.net

OrgTechHandle: ZV20-ARIN
OrgTechName: Verizon Internet Services
OrgTechPhone: 800-243-6994
<table>
<thead>
<tr>
<th>IP Information for 71.174.247.46</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>IP Location:</strong> United States Dedham Verizon Internet Services Inc</td>
</tr>
<tr>
<td><strong>Resolve Host:</strong> pool-71-174-247-46.bstnma.fios.verizon.net</td>
</tr>
<tr>
<td><strong>IP Address:</strong> 71.174.247.46</td>
</tr>
<tr>
<td><strong>Blacklist Status:</strong> Clear</td>
</tr>
</tbody>
</table>
Cookie Details

```
4071449904
30036801
*
WT_FPC
id=71.174.247.46-4051879904.30036801:lv=1256220204535:ss=1256220204535
microsoft.com/
1088
590536192
30771023
4073889904
30036801
*
MC1
GUID=51db8d5b3288d54a4cfd3d4ccad6e8d4d686d786d54a4
microsoft.com/
1024
2636615424
30771056
4076149904
30036801
*
A
I=&I=AxUFIAAAADBBwAAHmd22GNEydi6Ou26Cv+1Q!!
microsoft.com/
1024
1098813696
32240974
4076149904
30036801
```

Summary

- Privacy policies are prone to mistakes and equivalent to promises
- Not having the data, nor being able to get it, is privacy by design
- You are your data trail; increasingly others make decisions about you based upon your data trail.
Copyrights

- who uses tor?
  http://www.flickr.com/photos/mattw/2336507468, Matt Westervelt, CC-BY-SA

- danger!,
  http://flickr.com/photos/hmvh/58185411/sizes/o/, hmvh, CC-BY-SA

- 300k,
  http://flickr.com/photos/tochis/1169807846/sizes/, tochis, CC-BY-NC