Proxies, VPNs and Tor
What is hidden to some, is revealed to others.

Tim Sammut, @t1msammut
15 July 2015
Objectives

- Understand the differences
- Know when to use each
- Be mindful of challenges and pitfalls
Direct Communications
No precautions taken

Visible:
Everything*

* Ignores application-level encryption
Proxy Servers
Generally unencrypted communications through an intermediary

* Visible: Your IP Address
  Traffic contents*

That you are communicating with a proxy

* Visible: Everything*

Corporate environments utilize this visibility for logging and content inspection

* Visible: Your destination
  Traffic contents*

* Ignores application-level encryption
VPN Services – Internet

Encrypted tunnel to “trusted” location

Visible:
Your IP Address
That you are communicating with a VPN service

Visible:
Everything*

Visible:
Your destination
Traffic contents*

* Ignores application-level encryption
VPN Services – Corporate

Encrypted tunnel to a typical corporate network

Visible:
Your destination
Traffic contents*
That you are coming from corporate network

Visible:
Everything*
That you are communicating with a VPN service

Visible:
Your IP Address

* Ignores application-level encryption
Tor
Anonymization and near-side encryption

Visible:
Your IP Address
That you are using Tor

Visible:
Nothing

Visible:
Your destination
Traffic contents*

* Ignores application-level encryption
Use the right tool for the job.
And know no one tool can completely protect you.

<table>
<thead>
<tr>
<th></th>
<th>Direct</th>
<th>Proxy</th>
<th>VPN</th>
<th>Tor</th>
<th>HTTPS</th>
<th>TBB</th>
</tr>
</thead>
<tbody>
<tr>
<td>Censorship evasion</td>
<td>+</td>
<td>++</td>
<td>+++</td>
<td>+</td>
<td>+</td>
<td>+++</td>
</tr>
<tr>
<td>Make yourself appear elsewhere</td>
<td>+</td>
<td>++</td>
<td>+</td>
<td></td>
<td>+</td>
<td></td>
</tr>
<tr>
<td>Near-end encryption</td>
<td></td>
<td>++</td>
<td>+++</td>
<td>++</td>
<td>+++</td>
<td>++</td>
</tr>
<tr>
<td>Far-end encryption</td>
<td></td>
<td></td>
<td></td>
<td>++</td>
<td></td>
<td></td>
</tr>
<tr>
<td>End-to-end encryption</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>++</td>
<td></td>
</tr>
<tr>
<td>Anonymity</td>
<td>+</td>
<td>+</td>
<td>++</td>
<td></td>
<td></td>
<td>+++</td>
</tr>
<tr>
<td>Privacy</td>
<td>---</td>
<td>-</td>
<td>+</td>
<td>+</td>
<td>+</td>
<td>+++</td>
</tr>
<tr>
<td>Speed</td>
<td>+++</td>
<td>+</td>
<td>++</td>
<td>--</td>
<td></td>
<td>--</td>
</tr>
</tbody>
</table>

Use the right tool for the job.
And know no one tool can completely protect you.

Tor Browser Bundle
We know governments monitor us.

What about proxy, VPN and Tor operators?

What about governments leveraging these network locations with a high-density of “secretive” users?

*Every network is untrusted—act accordingly.*
Direct Communications
Pitfalls and Recommendations

If...

- You’re using a secure and robust protocol
- You’re not facing censorship
- Your network traffic will not trigger ramifications

...a direct connection may actually be the best option
Proxy Servers
Pitfalls and Recommendations

Outside of “corporate” environments, unless you have a very specific need, just don't use proxies.

VPNs are nearly-free, much less risky, and have stronger benefits.
If the task *does not require anonymity* and Tor is just too slow, VPNs are an option.

Very critical to select a reputable provider.
- Do they have a privacy policy?
- What geographies are they in?
- What governments have jurisdiction?
- Will their VPN client expose you to security issues?
VPN Services – Corporate

Pitfalls and Recommendations

Unless your association with “corporate” should remain secret, using the VPN is a good approach:

- Encrypts in-country traffic
- Circumvents local censorship and monitoring
- Corporate connection to the Internet relatively trusted

Make sure you are actually connected!
Real online anonymity is very difficult. If you require it you must use Tor Browser Bundle (TBB) or TAILS.

Don't do anything that would provide a link to your identity

- Don't connect to any site or service you use without TBB or TAILS
- If your use of Tor is a one-time occurrence, consider using TAILS from an unfamiliar location
Recommendations

- Treat every network as untrusted
- Use secure protocols everywhere
- To evade censorship and monitoring, use Tor together with secure protocols
Thank you.