Anomynity Course: Summary Document

Sean al-Baroudi

January 11, 2022

Glossary (Subset of):

-
-
-
-
-
-
-
-
-
-
-

1 Goals and Objectives / Intro:

1.1

- Understand how anonymity might be achieved against various adversaries.
- How to bypass censors (Firewalls, Proxies, DPI).
- Use of Live Operating Systems
- Virtual Private Networks
- Proxies, VPN and SSH
- I2P - Invisible Internet Project
- Different kinds of endpoints and networks, hotspits, cell networks, etc.
- Chaining anonymising services.
-

2 Operational Security (OPSEC):

2.1 Intro:

- To truely understand Anomynity online, one must understand Operational Security.
- Operational Security: OPSEC: The habits and behaviours one performs to enforce good security. Put another way, sloppy behaviours and exposure lead to security hazards that will get you compromised.
- Then OPSEC operationally and practically, can be seen as a set of best practices.
- **Anomynity (Ideal):** Keeping your actions **separate** from your identity. It doesn't mean your actions are hidden. Any distinguishing properties that might be inferred about your idenity are effectively hidden.
- **Pseudoanomynity:** Mapping your actions to a false identity or alias, which is removed from your true identity.
- It is very hard to separate our personal and professional identities - given how centralized our lives are around laptops and cellphones - they often blur.
- There are six main Identity Strategies for Separating your different identities, online:
  1. **Open Strategy:** Use your real identity and be honest. Only good for professional posting - must censor oneself in this instance.
  2. **Avoidance:** You can't make any exposure mistakes, but you miss out on content. Not often practical for long periods of time.
  3. **Audience Strategy:** You have a set of aliases, and each one maps to a different audience (example: Professional, Personal, Reddit/Twitter/Youtube, Side-Hustle, etc). This strategy cannot stop people that straddle audiences (example: work friends), from leaking material to other audiences.
  4. **(Acceptiable/PC) Content:** One alias for various audiences - you have to censor and maintain a consistent image (usually, the most safe) for all said audiences. Lack of Expression with this route.
  5. **Compartmentalization:** One identity for one audience - keep the ID's different enough so they can't be linked to one another. Drawback: A lot of overhead.
  6. **Custom Strategy:** Any practical mix of what is found above.
-
-

2.2 Establishing Cover / Identify Cross-Contamination:

- To establish cover, you must invent an entirely new identity, and embody it so it is believible.
- Start by going to *fakenamegenerator.com* to generate an identity.
- Create separate online accounts for hobby, personal and professional history. Link them together to generate the image of a person.
- Invest in the Image: Make posts, about this fictitious persons interests, set-up fake websites, steal pictures and post them. You need the life story of a person for people to follow.
- Note that the way you access the internet is just as big a fingerprint as your constructed activities. The following must be selected, and made consistent to avoid blowing your cover:

☐ Selection of Operating System, and Browser and device.
☐ Writing Style (Stylometry).
☐ Timezone and hours in which you post.
☐ Behaviours and kinds of posts.
☐ Dialects and spelling (regional)

- **Note:** If you can't afford separate machines for each identity - use Virtual machines on one device, at least.
- *You must access things in the same disciplined way, and behave in the same way. You are playing a character and must embody it fully.*
- **Checking if someone is looking at you:**

☐ Use Google Alerts+Keyword Analytics in-case someone posts about you, or looks you up.
☐ Search for your name in trackers and websites.

- Burning down a blown identity:
- Checkout the Removal Info Graphic for a list of things to remove.
- Certain websites respond to takedown requests, including Google, Youtube and Internet Archives.
- **Hiding if Discovered:**
- Each country has a list of extradition treaties - they are listed on Wikipedia.
-

2.3 Ten Rules of OPSEC:

1. Do not reveal methods or operational details.
2. Trust No One.
3. Never Contaminate Identities
4. Be Uninteresting
5. Be Paranoid Now: But remember they will take the easiest route to catch you - patch these first.
6. Know Your Limitations
7. Minimize Information
8. Be Professoinal
9. Employ Anti-Profiling
10. Protect Your Assets

2.4 Authorship Recognition and Evasion Methods

- Writing Style can be used to accurately narrow down a list of suspects. This field is called **Stylometry**
- With 5-6k words of text, an author can be ID'ed with 80 percent accuracy. More specifically, we can identify other pieces of work they wrote with about 80 percent accuracy.

- There are various style analysis tools one can use to see there own characteristics.
- There are online databases used by large organizations (Universities, Law Enforcement that use these methods).
- You can obscure this by embodying the writing style of others, or using anti-stylometry tools online. Quote others whenever you can, use leet/derp speak. Make intentional and repeated spelling and
- The easiest way to avoid Stylometry being used against you, is to not post large pieces of text.

3 Live OS - Tails, Knoppix, etc.

3.1

- Just install Tails or Knoppix. Can do it on a separate SSD or use a VMWare virtual machine.
- Use a VPN when you download these. You might be logged by a security agency.
-

4 Virtual Private Networks

For anonymizing services such as TOR, I2P, etc, VPNS are a relatively easy to use, but more vulnerable form of anomynity that one can implement.

4.1 Intro / Protocols:

- A Virtual Private Network is an encrypted connection that transmits data from a server to a client. A server (or chain of servers), will sit in front of a client, and will ideally (i) incrypt packet data between the client and destination and (ii) Hide the clients IP address from spying agents.
- VPN set up as follows:

$$Client \rightarrow (VPN_1) \rightarrow ... (VPN_K) \rightarrow Server_{dest}$$

- **Types of Configuration:**
☐ VPN client on local computer.
☐ VPN firmware on Router.
☐ Virtual Machine (with VPN client / router firmware inside).
- Your ISP can only see the connection between your computer and the first VPN in your chain.
- **VPN Protocols:**
☐ **PPTP:** Has a number of vulnerabilities - but is easy to set up.
☐ **L2TP + IPsec:** Layer Two Tunneling Protocol and Internet Security Protocol: These are coupled together to compensate for the weaknesses of each. L2TP doesn't provide encryption of traffic, and ISP does encrypt privacy. Easy to set up, but has fixed ports and is easy to block.
☐ **OpenVPN:** Can be configured to use TCP port 443 - so it looks like normal web traffic. Works faster over UDP. Not supported by most OSes by defualt - higher skill level needed to set this up. More secure than the other two types. Keys are Ephemeral (periodically change).
☐ **SSTP:** Secure Socket Tunneling Protocol: For windows only, made by Microsoft. Not open source - avoid.
☐ **IKEv2:** Internet Key Exchange. Developed by corporations - high performance but may be compromisd. Quick and Easy for Mobile Anomynity.
- Conclusion: Always choose OpenVPN if possible.

VPN Weaknesses / Who can you trust?

VPN Weaknesses:

- slower: negatively affected if its an international VPN, or chained. - single VPN not a solution to hide against a nation state, TOR and nested VPNs needed at the minimum. - not hidden from DPI - can be censored or blocked. - To evade VPN detection, stunnel or obsfproxy can be used. - If you sign up for a high performance VPN - you need to use anonymous forms of payment (crypto currency, Abine). - Vunlerble to end-to-end correlation attacks, if nation state has global surveillence. If a large adversary can observer the traffic going into a VPN network, and traffic going out, it can use correlation to associate data packets with anonymized users. - Cannot protect you against direct attacks on the final destination - these could be compromized. - Occasional VPN usage can be a fingerprint to attacker, when you are doing sensitive work! - Many common VPN providers are autoblocked (Netflix, 4Chan). - VPNs don't harden your browser - so cookies and fingerprinting can be. - VPNs are a tool for privacy - not anomynity. People can still guess who you are (with a lot of work), but they can't see the content. what your encrypted data streams

Can you trust VPN providers:

- No. They are a man in the middle by definition. - You can mitigate this with chaining and using different providers. - Warrant Canaries: Providers issue a statement saying they have not been served a warrent. When the statement is removed, they are compromised. Actor can still lie, or government can force them to keep it up with coersion - a nice gesture but not a reliable signal. - EU has data retention laws, US does not. Legal VPN providers must abide by the geopolitical rules they have. - A company could roll over for a government at any time. Which countries should you pick? - Bulgaria, Cyprus, Iceland, Romania, Serbia.

- Avoid Totalitarian/Authoritarian/Muslim governments, Five Eyes, Commonwealth, US.

VPN and DNS Leaks: - DNS resolves domain names to an IP address. - If DNS can't be resolved by local cache, we use a DNS server. - Router is given Primary DNS server by ISP. - You can choose your DNS that is open and is focused on privacy. - Port: UDP/TCP: 53 (plaintext, unencrypted!). - Even with using your own DNS, ISP can use a transparent proxy to intercept all DNS requests and forward them to their servers. - Use DNS leak tests to see if the DNS resolved is what you selected. - Risk: DNS Poisining/Spoofing (government and hackers - for censorship and hijacking).

OpenVPN Setup (Linux):

A few types of files: - ovpn config files - key and certificate files to set up encrypted connections. - You need to set this out ***

VPN Data Leaks: There are a number of reasons why data can leak from a VPN:

1) VPN Disconnect/Drop: Your connection can terminate - your computer will use other connections to try and push network traffic. You will be immediately exposed if this is not clamped down (VPN connection only). 2) IPv6 Data Leaks: This protocol is not used much - your IPv4 may be secure, but if your system chooses to send packets with ipV6, you are completely exposed. 3) Transparent DNS Proxies: Your provider will reroute your DNS queries before it hits your first VPN server, and you will be exposed.

How to stop it: - Disable ipV6 for your OS! - We must block all non-VPN traffic, incase our connection drops. You can use a Killswitch in a VPN client. - Use host based firewalls to block VPN leaks. - Linux: VPNDemon and VPN Firewall, IP Tables to block non-VPN traffic.

Choosing the Right VPN Provider: - anonymous payments (crypto), and no KYC. - chosen based on your adversary (local hacker, or world government). - Countries not apart of mass surveilence, Commonwealth, or with Authoritarian/Totalitarian/Arab governments. - Countries: Bulgaria, Cyprus, Iceland, Romania, Serbia, Switzerland. - not registered in a hostile country. - no external support services (risk of social engineering). - prevents DNS and VPN leaking (see above) - hardened servers, controls own servers. Not runnning other serivces (HTTP, FTP, etc). - minimial logging.

4.2

-
-
-
-
-
-
-
-
-
-
-
-
-
-
-
-
-
-

12 Chaining / Nesting Privacy and Anonymising Services:

12.1

13 Offsite Connections - Hotspots and Cafes:

13.1

14 Mobile, Cell Phone and Cell Networks:

14.1

15 Wrap-up:

15.1

16 Bonus Content:

16.1

17

17.1

References

[1] https://purple.com

[2]

[3]

[4]

[5]

[6]