Anonymity and Attribution in Cyberspace and the Dark Web

CS-3113: PRINCIPLES OF CYBER SECURITY

BENJAMIN R. ANDERSON

Accountability in Cyberspace

Watch: *Accountability in Cyberspace: The Problem of Attribution* from the RAND Corporation

- https://www.rand.org/multimedia/video/2019/01/14/accountability-in-cyberspace-the-problem-of-attribution.html
- Make a note of the three types of indicators for attribution (technical, political, clandestine)
- The same indicators that could attribute an attack could be used by a nation state to impersonate another country
  - A variant of a “false flag” operation

Anonymity Vs. Privacy

These are ***not*** the same thing

Read: In Cyberspace, Anonymity and Privacy are Not the Same, Adam Firestone

- https://www.securityweek.com/cyberspace-anonymity-and-privacy-are-not-same

From the article:

- *Unfortunately, many of the privacy grievances stem from the frequent conflation of privacy with anonymity. The two are qualitatively, and legally, different, but confusion about this likely comes from the Internet's original architecture, which placed great value on the reliability and robustness of communications, but less emphasis on identity management and security. As a result, we are living under the mythos of entitled anonymous Internet communication and activity.*

  Privacy, according to the Merriam-Webster Dictionary, is "the state of being alone" or "the state of being away from other people." It's about being able to reach a place of sanctuary where one is free from unauthorized intrusion or public attention. The same resource defines anonymity as "the quality or state of being unknown to most people" or "the quality or state of being anonymous." The two are clearly different. Privacy is the ability control what one discloses to whom and when, while anonymity is about one's interactions with an environment of which one is part, but which one does not own or control.

Free Speech Issues

The issues around anonymity and privacy on the internet are not technical in nature

- They are in the legal and ethical realm

From Harvard University:

- *Anonymity on the Internet- Protection of Free Speech or Shield for Abuse?*
  - *There are many ways to communicate anonymously on the Internet, including anonymous remailers for e-mail, anonymous posting, and anonymous creation of Web pages. Anonymity allows a person to express his or her views freely, without the fear of repercussions. Anonymity allows a person to be controversial, to take unpopular positions on volatile issues, to try to change society. The Internet allows an individual with no money potentially to reach a large audience and make a real impact. But this forum can also be abused. People can post someone else's private information on a Web site anonymously. People can write untrue or damaging statements anonymously. Do you think anonymity on the Internet should be protected?*
  - *https://cyber.harvard.edu/lesson7/anonymity.html*

Free Speech Issues: Court Cases

ACLU v. Miller, Northern District, Georgia, ACTION 1:96-cv-2475-MHS

In ACLU v. Miller, the American Civil Liberties Union got an injunction against the enforcement of a Georgia statute that prohibited a person from falsely identifying herself while sending e-mail, posting on the Internet, and more (one of the problems with the statute was that it was too vague). The court ruled it was appropriate to give an injunction, among other reasons, when there was the potential for chilling free expression. The court agreed with the state that its purpose in enacting the statute--preventing fraud--was a compelling state interest, but decided against the state because the statute was not narrowly-enough tailored to its purpose.

- *https://cyber.harvard.edu/lesson7/anonymity_cases.html*

Talley v. California, 362 U.S. 60 (1960)

This case dealt with a Los Angeles city ordinance which required distributors of leaflets to fully identify themselves and provide a mailing address. A group called the National Consumers Mobilization urged a boycott of certain merchants because of their "discriminatory" policies. The group disbursed handbills which did not meet the requirements of the ordinance governing anonymous leaflets and the person responsible was subsequently arrested and fined. The Supreme Court struck down the ordinance and held that it unduly abridged the freedom of speech guaranteed by the First Amendment. The Court reasoned that the ability to anonymously distribute ideas goes to the core of free speech. The Court stated that anonymity has furthered freedom of expression throughout American history by allowing persecuted individuals and groups to disseminate their viewpoints.

- *https://cyber.harvard.edu/lesson7/anonymity_cases.html*

Free Speech Issues: Court Cases

McIntyre v. Ohio Elections Commission, Syllabus, US Supreme Court, cert to Supreme Court of Ohio, No. 93-986, 1995

- *This is another case dealing with anonymously distributed pamphlets and an attempt by government officials to require identification on all such material. A pamphleteer distributed anonymous leaflets opposing a school tax levy and was subsequently fined by the Ohio Elections Committee for violating a statue requiring self-identification. The Court of Common Pleas reversed the decision to impose a fine. The Court of Appeals reinstated the fine and the Ohio Supreme Court affirmed the decision. Finally, the Supreme Court of the United States struck down the fine, on reasoning similar to that in Tally. The Court held that the ability to publish anonymously is guaranteed under the First Amendment unless a prevailing governmental interest overrides concerns for liberty.*
- *https://cyber.harvard.edu/lesson7/anonymity_cases.html*

Does the U.S. Supreme Court have jurisdiction in cyberspace?

- If all the systems are in the U.S. – almost certainly
- What about if the servers are in Germany?
- What about if the servers are in the U.S. but the individual is in Germany?
- What about in the middle of the ocean, or in space?

Anonymity and Attribution

From: *The Decision to Attack* by Aaron Franklin Brantly, Chapter 5

- *Anonymity and, by extension, attribution are two fundamental aspects of the cyber domain. When a state decides to attack another state, it is not concerned solely with its relative power to its adversary. An attacking state is concerned with the power of its adversary and its ability to conduct an attack against an adversary while maintaining anonymity. Anonymity in cyberspace in the initiation and implementation phases of an attack provides the freedom to maneuver. Webster's defines anonymity as follows:*
  - *Of unknown authorship or origin*
  - *Not named or identified*
  - *Lacking individuality, distinction, or recognizability*
- *The analysis [in the chapter] focuses on the origin or instigating actor, the target that is not identified, and the recognition that an attack is occurring. Specifically the concept of anonymity is approached from the offensive perspective of a state considering instigating a cyber attack against a potential opponent.*

Politics also comes into play when dealing with attribution

From: *The Decision to Attack* by Aaron Franklin Brantly, Chapter 5

- *To understand anonymity it is necessary to ask basic questions of international politics.*
  - *Why is anonymity important to a cyber attacker?*
  - *Is it possible to conduct a political act and remain anonymous?*
  - *Why is attribution important to a cyber defender?*

From: *The Decision to Attack* by Aaron Franklin Brantly, Chapter 5

Anonymity and Attribution

Most of the literature on cyber attacks makes clear that one of the most valuable aspects of the cyber domain is anonymity.

Anonymity is a distinctive asset in covert operations, providing political plausible deniability while allowing for the attainment of a strategic or tactical objective.

It is difficult to assess the true value of anonymity in cyber. From an offensive perspective the objective is to remain anonymous as long as possible while still achieving an objective.

- *This is likely to lead an attacker to obfuscate his or her operation.*
- *…if a target of a potential attack emanating from cyberspace know where an attack will occur, or who will perpetrate an attack, it is much more likely to be able to defend against that attack.*

Anonymity in cyber is multifaceted. The layers of anonymity are constructed by the following characteristics:

- *The inability to identify a perpetrator (state instigator) of an attack,*
- *The inability to recognize an attack is occurring, and*
- *The inability to isolate the target or objective of an attack.*

Beyond simply being unable to identify the perpetrator, as is often the case in cyber attacks, it is difficult to recognize when a cyber attack is

From: *The Decision to Attack* by Aaron Franklin Brantly, Chapter 5

Politics and Remaining Anonymous

If we follow the logic of Thomas Rid that 'history does not know acts of war without eventual attribution,' then do cyber attacks constitute political acts? With anonymity being a central feature that influences the success of cyber attacks, does anonymity remove the political aspect of attacks? Rid goes on to say: 'aggressors engaging in subversion, espionage or sabotage do act politically; but in sharp contrast to warfare, they are likely to have a permanent or at least temporary interest in avoiding attribution. This is one of the main reasons why political crime, more than acts of war, has thrived in the cyber domain, where non-attribution may be easier to achieve than waterproof attribution.'

What is evident is that regardless of how cyber attacks are referred to in the conventional typology, they are capable of generating utility.

From: *The Decision to Attack* by Aaron Franklin Brantly, Chapter 5

Attribution and Cyber Defense

An anonymous actor is one who avoids attribution.

The ability for states to respond to cyber attacks and their perpetrators is an important aspect of cyber defense.

When we consider the offensive strategy of a state, the concern is a combination of achieving the objective and avoiding attribution. For an attack to gain political utility, a state must achieve its stated objective. If a state cannot achieve even the minimum threshold of its objective, an attack remains unattributed if it did not gain any political utility.

Attribution is a fundamental aspect of cyber defense.

Once a targeted country begins the attribution process, it is often after an attack has been completed.

Deterrence does not work the same in cyber as in conventional conflict. Simply identifying the attacker and threatening response is typically not possible. And even when it is possible, it is only feasible with a cross-domain response. Such a response would likely escalate a conflict significantly with unforeseen consequences.

From: *The Decision to Attack* by Aaron Franklin Brantly, Chapter 5

Attribution Can Be A Secondary Priority

The scenario is one in which the previously laid groundwork for a coordinated attack against U.S. critical infrastructure begins to take down vital U.S. systems coinciding with a foreign policy flap occurring with China.

The decision-makers are paralyzed because at first it is not known whether the critical infrastructure malfunctions are due to an attack or normal error.

As the malfunctions continue to occur, it becomes apparent the malfunctions are due to an attack and not an error. Although the likely attributable source is China, that is of little importance.

The anonymity of the attack and the targets of the attack are more important than pointing fingers… by the time it was recognized as an attack it was too late to do anything, let alone isolate future targets, and the United States didn't have assets in place to retaliate in kind.

….a cross domain response would have been a prelude to all-out war with unforeseen consequences between two nuclear-armed states.

Moreover, to publicly attribute the system failures within the U.S. critical infrastructure without having a means to stop them also has many negative side effects…. It could severely degrade public confidence in critical infrastructure and cause widespread panic.

From: *The Decision to Attack* by Aaron Franklin Brantly, Chapter 5

The Dark Web

You have probably heard about the “Dark Web” in advertising for credit monitoring services

However, you may not be familiar with what exactly that means

Here are some key definitions:

Surface Web: The Surface Web (also called the Visible Web, Clearnet, Indexed Web, Indexable Web or Lightnet,) is that portion of the World Wide Web that is readily available to the general public and searchable with standard web search engines.

Deep Web: The deep web, invisible web, or hidden web are parts of the World Wide Web whose contents are not indexed by standard search engines for any reason. The opposite term to the deep web is the surface web. The deep web includes many very common uses such as web mail and online banking but also paid for services with a paywall such as video on demand, and many more.

- For example, a shared folder that doesn’t have a link from a web page, so a search engine never finds it and indexes it

Dark Web: The dark web is the World Wide Web content that exists on darknets, overlay networks which use the public Internet but require specific software, configurations or authorization to access. The dark web forms a small part of the deep web, the part of the Web not indexed by search engines, although sometimes the term "deep web" is mistakenly used to refer specifically to the dark web.

Darknet: A darknet (or dark net) is an overlay network that can only be accessed with specific software, configurations, or authorization, often using non-standard communications protocols and ports. Two typical darknet types are friend-to-friend networks (usually used for file sharing with a peer-to-peer connection) and privacy networks such as Tor.

Definitions from Wikipedia

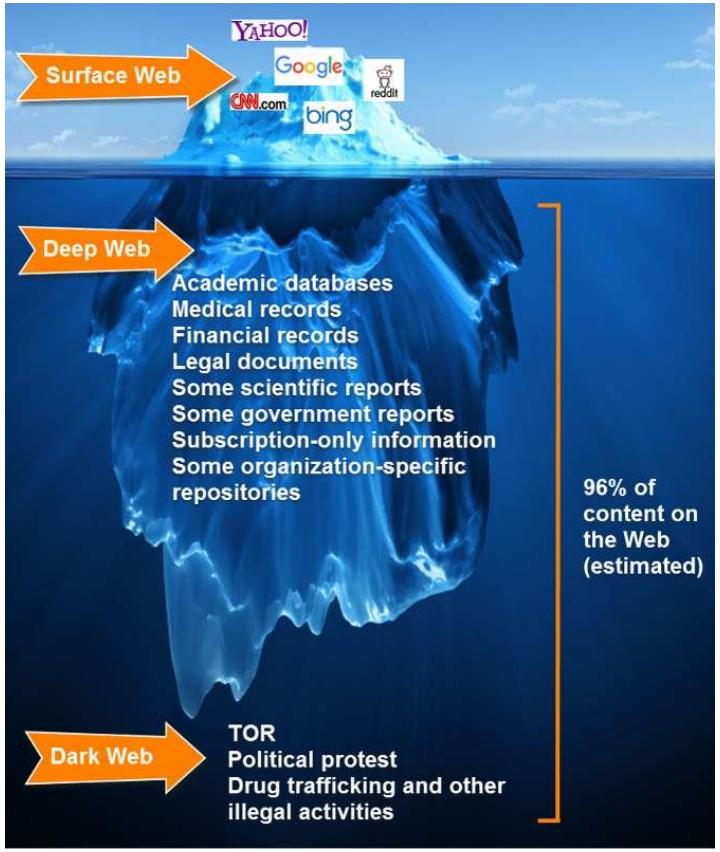
The Dark Web

Conceptually, we can think of this as an iceberg

- While there are many services that are in “open view” there are far more that are not
- It requires specialized software to access
- For example, you can use an alternate browser (like Tor) to access this content

The Dark Web has been around for decades and has many purposes (besides criminal)

- It can allow legitimate individuals who need to remain anonymous (ex. intelligence agents) to communicate
- Can allow for debate on controversial topics without fear of retaliation
- Provides a venue where individuals with little resources can freely communicate and have a large impact with their ideas



The Dark Web

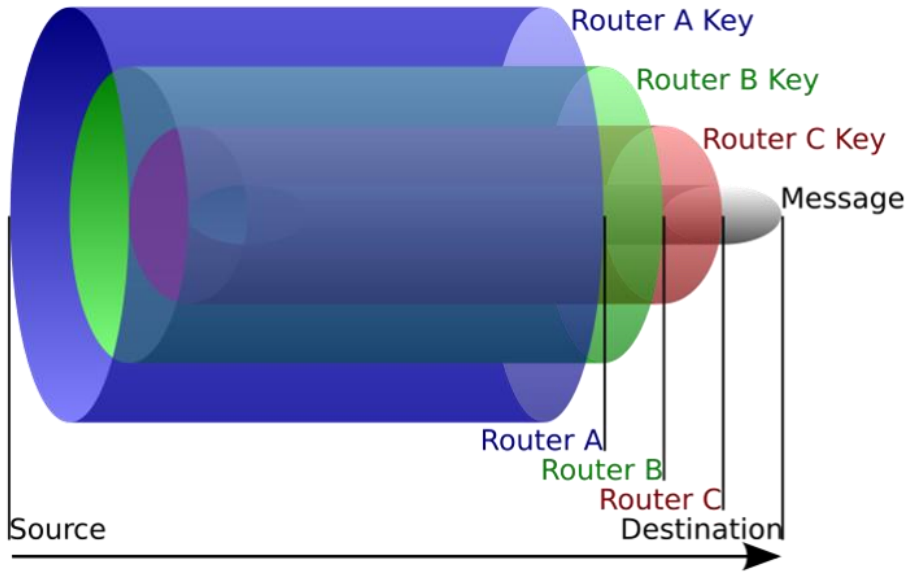
Read: *The Darknet: A Short History* by Ty McCormick

- https://foreignpolicy.com/2013/12/09/the-darknet-a-short-history/
- You do not need to memorize dates, just get a feel for the timeline
- Also, note that Bitcoin was quickly adopted by sites on the Dark Web

Onion Routing

Remember how onion routing works

- Onion routing is an hybrid link encryption approach
- A routing onion (or just onion) is a data structure formed by 'wrapping' a plaintext message with successive layers of encryption, such that each layer can be 'unwrapped' (decrypted) like the layer of an onion by one intermediary in a succession of intermediaries, with the original plaintext message only being viewable by at most: the sender, the last intermediary, and the recipient. (If end-to-end encryption is also used, then only the sender and the recipient.)

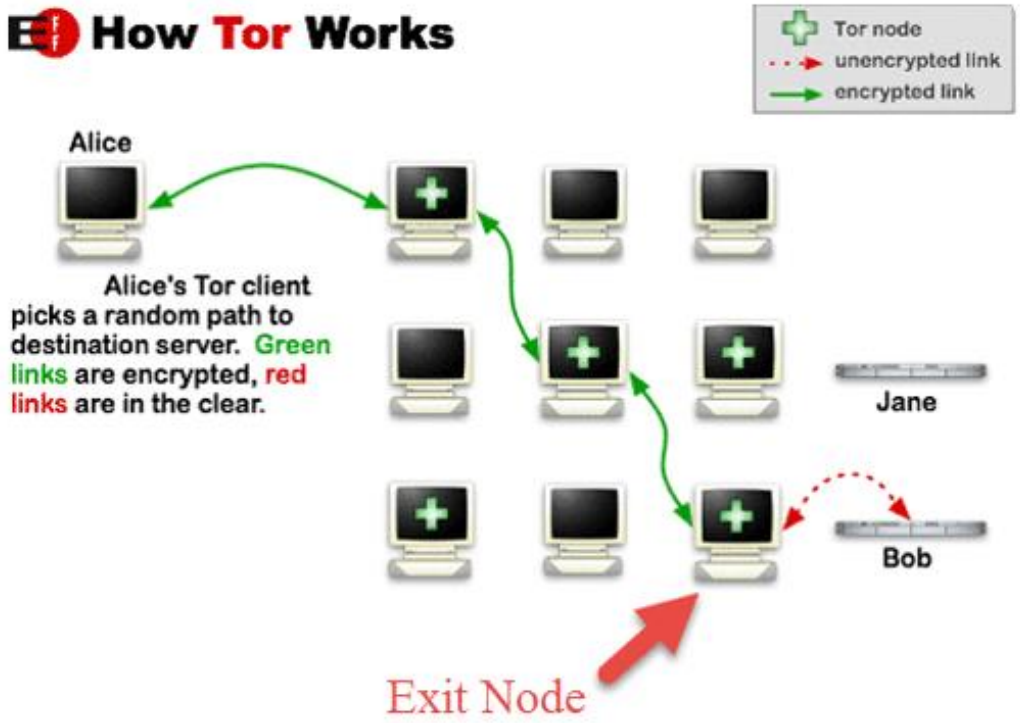


Onion Routing

The Tor Browser uses onion routing

Read: *This Is How Tor Protect Your Anonymity On The Internet* by Sara Aftab

- https://wonderfulengineering.com/this-is-how-tor-protect-your-anonymity-on-the-internet/
- *It should be noted, however, that Tor doesn't offer complete end-to-end encryption. It offers encryption from the sender to the last relay, and then that relay will send the data unprotected to its final destination. In the case that that exit node is malicious, then all unencrypted data that Tor sends through that relay could be intercepted. Hence while Tor makes the tracking difficult, is does not make it impossible. In practice, it is a good idea to periodically change circuits, or to combine use of Tor with the use of Virtual Private Networks (VPNs). Another point to consider here is that routers can be manipulated for anonymity while bridges cannot be. Tor does nothing to prevent the leak information when it comes to the storage of cookies or use of javascript. Therefore, accomplishing complete anonymity using Tor alone may not be the ultimate solution.*



Tor Vulnerabilities

There are multiple vulnerabilities inherent in Tor

- Some rely on malicious nodes that provide an attacker (or government) with information about the connections they see
- Some are only possible for large ISPs
  - For example, what if AT&T decided to delay all Tor traffic using its transatlantic cables for 10 seconds
  - An entity monitoring Tor traffic could see the delay and know that the routing for a specific went over that link, allowing it to start tracing the origin

Read: *Tor (network)* on Wikipedia, the Weaknesses section:

- https://en.wikipedia.org/wiki/Tor_(network)#Weaknesses
- Make note that the Heartbleed OpenSSL bug took down the Tor network for several days
- The network needed time to regenerate the private keys

If you want better security than Tor can provide, add a VPN with the server so your message is still encrypted when it leaves the Tor network

The Dark Web Marketplace

What is on the Dark Web:

- There are many goods and services that can be found on the Dark Web:
  - Malware
  - Intelligence information
  - Compromised user credentials
  - Criminal services (Ransomware-as-a-service)
- ***Read***: *What is the dark web? How to access it and what you'll find*, by Darren Guccione
- https://www.csoonline.com/article/3249765/what-is-the-dark-web-how-to-access-it-and-what-youll-find.html

From the article:

- Make note of what's available on the dark web
- How to access the dark web
- How to locate resources
- How financial transactions work

Dark Web Example: Silk Road

Silk Road was the first major black market on the dark web

- Essentially the Amazon of the dark web
- Although it only had customers numbering around 100,000

Read: Silk Road (marketplace) on Wikipedia:

- https://en.wikipedia.org/wiki/Silk_Road_(marketplace)
- Make note of what happened to Ross Ulbricht (Silk Road 1) and the administrators of Silk Road 2.0
- ***Hint***: They were all arrested
- See the diagram for how sophisticated the Silk Road payment system is