Internet Geolocation: An Adversarial Perspective

AbdelRahman M. Abdou*. Advisors: Dr. Matrawy*, Dr. van Oorschot†

*Systems and Computer Engineering, †School of Computer Science, Carleton University

Carleton UNIVERSITY

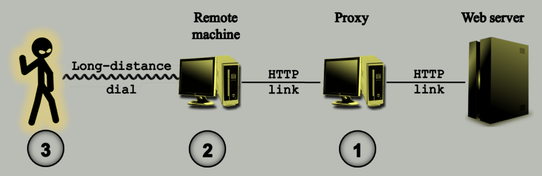
Abstract

We are exploring Internet geolocation from an adversarial perspective. The adversary is an end client trying to evade geolocation. We consider adversaries' motivations to circumvent geolocation, and mention two evasion objectives. We summarize evasion tactics, current geolocation techniques and their vulnerability to evasion.

Geolocation: Objectives and Techniques

A geolocation technique should aim to [1]:

1. Geolocate the IP address of the client seen at the server side.
2. Geolocate the actual device used for requesting a service.
3. Geolocate the end client (human) visiting a web server.



Current geolocation techniques include [1, 2]:

- Information registered in DBs or leaked.
- Information submitted.
- Delay-based approaches.
- Topology-aware approaches.
- W3C geolocation API:
  - IP address to location databases (Akamai, Digital Envoy, MaxMind, Quova, Verifia, etc.)
  - WPS (`Skyhook` and `Google`).
  - GPS (supported by smart phones).
  - Cell tower triangulation.

Evasion: Definition, Motivations and Objectives

We define the evasion of geolocation as:

"Causing the geolocation technique to fail or to return an incorrect location"

Motivations for evading geolocation techniques are:

- Misrepresenting location to gain location-dependent benefits.
- Avoiding accountability.
- Preserving privacy.

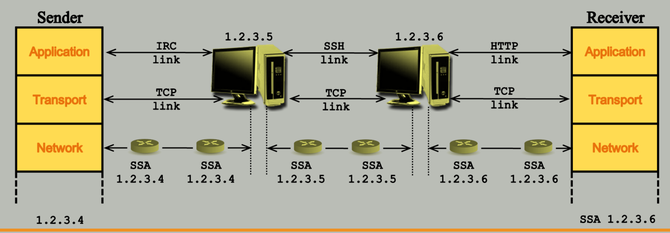
Adversaries usually defeat geolocation techniques by aiming to:

- Conceal their actual location.
- Virtually move themselves to another forged location.

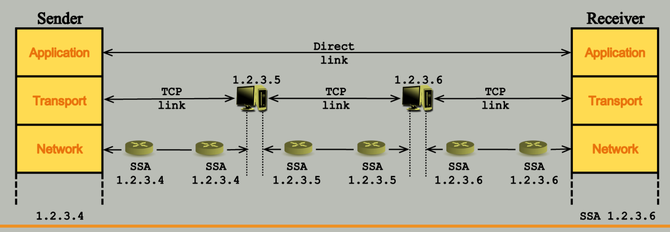
Evasion Tactics

In the evasion tactics below, tactics (2) and (3) aim to circumvent delay-based and topology-aware techniques. Tactic (5), which is apparently simpler, attempts to have the geolocation technique identify the location of a stepping-stone or a proxy node, rather than that of the end client. In addition, note that tactic (3) requires a *"sophisticated"* adversary that has control over multiple geographically distributed nodes [3].

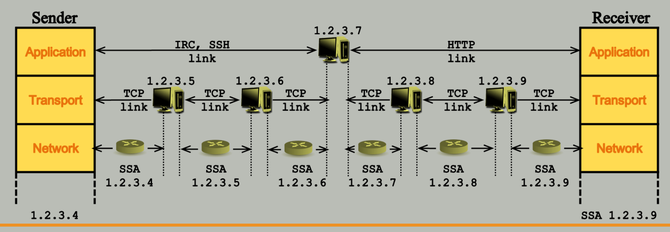
1. Submitting false information.
2. Blocking/delaying ICMP packets.
3. Spoofing hops along the path to the target [3].
4. Forging the returned GPS, WPS and/or cell tower triangulation coordinates that are sent back to a server.
5. Using one or more stepping-stones (an intermediate relaying agent between a client and a server) while connecting to a server:
   - Application-layer stepping-stones (E.g.: `SSH`ing into a remote machine and connecting to a web server from the remote machine, application-layer proxies, etc):



   - Transport-layer stepping-stones (E.g.: anonymizing browsers, transport-layer proxies, etc):



   - Application and transport layers stepping-stones (E.g.: `SSH`ing into a remote machine through a proxy and using `Tor` [4] from the remote machine to connect to a web server):



Matching

In the following table, the rows represent the geolocation techniques whereas the columns represent the evasion tactics discussed earlier (at the *"Evasion Tactics"* section on the left). A check mark (✓) at a cell in row *i* and column *j* means that the geolocation technique at row *i* can be evaded by the tactic in column *j*.

Geolocation Techniques \ Evasion Tactics		(1)	(2)	(3)	(4)	(5)
Information registered in DBs or leaked*		✓				✓
Information submitted		✓				
Delay-based approaches			✓	✓		✓
Topology-aware approaches			✓	✓		✓
Geolocation API	IP address DBs					✓
	WPS**	✓			✓	
	GPS**				✓	
	Triangulation**				✓	

* By "information leaked", we mean any information conveyed by the network or by a user application that aids in geolocating a user. Examples would be country codes or city names in domain names, HTTP headers showing time zones, etc.

** Those three techniques don't rely on network-transmitted measurements nor IP addresses. They send location information to the server directly (or other information that the server uses to recognize the location).

Conclusion

As can be seen, all studied geolocation techniques (listed in the table) can be evaded by a knowledgeable adversary who is aware of the techniques being used. Both delay-based and topology-aware techniques can be evaded, not only to an extent where an adversary conceals its actual location, but also by virtually moving itself to a specific forged location [3]. Our plan is to devise new Internet geolocation techniques that are robust to adversarial evasion.

References

J. Muir and P. C. van Oorschot, "Internet geolocation: Evasion and counterevasion," *ACM Comput. Surv.*, vol. 42, no. 1, Dec. 2009.

E. W. Nick Doty, Deirdre K. Mulligan, "Privacy issues of the W3C geolocation API." [Online]. Available: http://escholarship.org/uc/item/0rp834wfr

P. Gill, Y. Ganjali, B. Wong, and D. Lie, "Dude, where's that IP?: circumventing measurement-based IP geolocation," in *Proceedings of the 19th USENIX Security Symposium*, 2010.

"The Tor project." [Online]. Available: https://www.torproject.org/