User Location Verification on Internet

Deepika. K
Department of CSE,TRP
Engineering college,trichy,India

Preethi. P
Department of CSE,TRP
Engineering college,trichy,India

Pavithra. P
Department of CSE,TRP
Engineering college,trichy,India

***Abstract*- A number of services in internet require the user's location. This is mainly done for some security purposes. Few internet services are in need of the user's geographical locations when they access these services. Intruders can easily escape the existing geo location techniques. This is done by faking the GPS co – ordinates or employing a dynamic IP address through proxy and VPNs. In this paper, a novel technique called User Location Identification (ULI) is introduced to verify a user's location prescribed in a geographic location. This technique doesn't identify the users by their IP addresses. HTML5 Geo location can be implemented if the user's device is a mobile device with GPS or GPS like triangulation features. This will give much more accurate information than the Geo – IP address. If the user's device does not use GPS it may alternatively influence the local SSID information and compare with other datasets to verify its physical location. This prevents an intruder from manipulating delays. ULI reduces the opportunity of intruders by implementing one –way application delay from or to the user's device and evaluates these delays as a proof for locating the user's location. This approach is implemented in social networks like Facebook, Twitter or Instagram and the various factors like efficiency, location, user's access time are evaluated. Experimental results show that ULI predicts the user's location in an effective manner.**

1. INTRODUCTION

The Internet connects hosts from all across the world. Sometimes it is desirable to know where, geographically, a particular host is. Informally, Internet geolocation is the problem of determining the physical location (to some level of granularity) of an Internet user. A related but more specific term is IP geolocation, which refers to the problem of locating an Internet host using only its IP address. A growing number of companies (e.g., Akamai, Digital Envoy, MaxMind, Quova, and Verifia) now maintain and license databases which map IP addresses to geographic locations. The development of Internet geolocation technology is being driven by a number of applications; among the most lucrative is targeted advertising: if a host serving a Web page is able to determine that a visiting client is in, say, Seattle, then the server can embed in that page advertisements targeted to Seattle customers (e.g., umbrellas). Other suggested applications of Internet geolocation include automated redirection to nearby servers and Web analytics (i.e., analyzing Web page access logs to extract marketing data).

Web sites often tailor content (other than advertisements) based on geographic location. For example, content served by Google undergoes automated country redirection based on client IP address. Faced with an ever increasing amount of unwanted traffic, Internet services must be able to differentiate clients in order to enforce access-control decisions. One traditional approach is to use the client's IP address as an identifier. For instance, if a client is exhibiting malicious behavior— such as attempting to post spam messages to online blogs or trolling ssh servers for weak passwords—a server may add the client's IP address as a firewall rule that will prohibit further connections from the offending address. Unfortunately, middleboxes (both layer-3 network address translation (NAT) devices and layer-5 proxies) and dynamic IP renumbering due to DHCP challenge the utility of using IP addresses as client identifiers. Given the previous example, adding a firewall rule for an IP address due to abusive behavior (blacklisting) can deny system access to many users that may share that IP, either simultaneously via a middlebox or over time via DHCP. Similarly, when IP addresses are naively used to allow access to a resource (white listing), an open proxy from an authenticated domain, such as a university, can enable Internet-wide access to the protected resource.

The phenomenon of edge technologies obscuring a client's identity at the network level as edge opacity. Due to these apparent operational issues, many websites have moved from using IP addresses as identifiers to requiring some form of registration, authentication and then application-level identity checks. For example, it is not uncommon for wikis or web forums to require their users to register, login, and then present HTTP cookies on each access. Yet, these extra steps can be a usability hurdle and generally require more server-side resources. Because of these concerns, other websites continue to use IP white listing and blacklisting as the basis for managing client access. And yet, as the extent of edge opacity remains unquantified, the impact of using IP addresses as client identifiers is uncertain. Thus, server operators are making uninformed decisions regarding the best way to use IP addresses as client identities.

Over the Internet, Location-Sensitive Providers (LSPs) are those that customize their content/services based on the geographic locations of their clients (the software that communicates with the LSP, typically a web-browser). Some LSPs restrict their services to certain geographic regions, such as media streaming (e.g., hulu.com); others limit certain operations to a specific location, such as online voting (e.g., placespeak.com), online gambling (e.g., ballytech.com), location-based social networking (e.g., foursquare.com), or fraud prevention (e.g., optimal payments. com). LSPs may also use location information as an additional authentication factor to thwart impersonation and password-guessing attacks (e.g., facebook.com).

Privacy laws differ by jurisdiction, which allows/bans content based on region. The nature of the provided services may motivate clients to forge their location to gain unauthorized access. Existing geolocation technologies, commonly used in practice, are susceptible to evasion. For example, the W3C geolocation API defines an interface that allows the client's web browser to determine and return the client's location to the requesting LSP. Browser vendors usually rely on common location-determination technologies, such as Global Positioning System (GPS) or Wi-Fi Positing System (WPS). Because the client sends its location to the LSP, it can submit forged location information. Tabulation-based techniques, where a geo location service provider maintains tables that map IP addresses to locations—e.g., MaxMind, can be evaded through IP address-masking technologies such as proxy servers and anonymizers. Geolocation that is based on active delay measurements is prone to an adversary corrupting the delay-measuring process.

A location verification technique is therefore required to provide greater assurance of the veracity of the specified location. Various solutions have been proposed to verify location claims in wireless networks. However, solutions in this domain cannot be directly adopted by multi-hop networks, e.g., the Internet, due to delay characteristics of different domains. For example, Internet delays are stochastic, whereas in single-hop wireless networks, delays can be estimated from the distance the signal spans and the speed of its propagation. Verifying the location of Internet clients is a challenging problem. A practical approach must address critical challenges such as handling of IP address-masking, and ensuring the correctness of location information submitted by the client.

1.1 Title: Accurate One-Way Delay Estimation With Reduced Client-Trustworthiness

The requirement for accurate one-way delay (OWD) estimation lead to the recent introduction of an algorithm enabling a server to estimate OWDs between itself and a client by cooperating with two other servers, requiring neither client clock synchronization nor client trustworthiness in reporting one-way delays. We evaluate the algorithm by deriving the probability distribution of its absolute error, and compare its accuracy with the well-known round-trip halving algorithm. While neither algorithm requires client-trustworthiness nor client clock synchronization, the analysis shows that the new algorithm is more accurate in many situations.

1.2 Title: Dtrack: A System To Predict And Track Internet Path Changes

In this paper, we implement and evaluate a system that predicts and tracks Internet path changes to maintain an up-to-date network topology. Based on empirical observations, we claim that monitors can enhance probing according to the likelihood of path changes. We design a simple predictor of path changes and show that it can be used to enhance probe targeting. Our path tracking system, called DTRACK, focuses probes on unstable paths and spreads probes over time to minimize the chances of missing path changes. Our evaluations of DTRACK with trace-driven simulations and with a prototype show that DTRACK can detect up to three times more path changes than traditional trace route-based topology mapping techniques.

1.3 Title: Network Measurement Based Modeling And Optimization For Ip Geolocation

IP geolocation plays a critical role in location-aware network services and network security applications. Commercially deployed IP geolocation databases may provide outdated or incorrect location of Internet hosts due to slow record updates and dynamic IP address assignment by the ISPs. Measurement-based IP geolocation is used to provide real time location estimation of Internet hosts based on network delays. This paper proposes a measurement-based IP geolocation framework that provides location estimation of an Internet host in real time. The proposed frame work models the relationship between measured network delays and geographic distances using segmented polynomial regression model and semi definite programming for optimization. Weighted and non-weighted schemes are evaluated for location estimation. The proposed framework shows close to 17 and 26 miles median estimation error for nodes in North America and Europe, respectively. The proposed schemes achieve 70–80% improvement in median estimation error comparing to the first order regression approach for experimental data collected from Planet-Lab.

1.4 TITLE: PEERING THROUGH THE SHROUD: THE EFFECT OF EDGE OPACITY ON IP-BASED CLIENT IDENTIFICATION

Online services often use IP addresses as client identifiers when enforcing access-control decisions. The academic community has typically eschewed this approach, however, due to the effect that NATs, proxies, and dynamic addressing have on a server's ability to identify individual clients. Yet, it is unclear to what extent these edge technologies actually impact the utility of using IP addresses as client identifiers. This paper provides some insights into this phenomenon. We do so by mapping out the size and extent of NATs and proxies, as well as characterizing the behavior of dynamic addressing. Using novel measurement techniques based on active web content, we present results gathered from 7 million clients over seven months. We find that most NATs are small, consisting of only a few hosts, while proxies are much more likely to serve many geographically distributed clients. Further, we find that a server can generally detect if a client is connecting through a NAT or proxy, or from a prefix using rapid DHCP reallocation. From our measurement experiences, we have developed and implemented a methodology by which a server can make a more informed decision on whether to rely on IP addresses for client identification or to use more heavyweight forms of client authentication.

1.5 Title: Internet Geolocation: Evasion And Counterevasion

Internet geolocation technology aims to determine the physical (geographic) location of Internet users and devices. It is currently proposed or in use for a wide variety of purposes, including targeted marketing, restricting digital content sales to authorized jurisdictions, and security applications such as reducing credit card fraud. This raises questions about the veracity of claims of accurate and reliable geolocation. We provide a survey of Internet geolocation technologies with an emphasis on adversarial contexts; that is, we consider how this technology performs against a knowledgeable adversary whose goal is to evade geolocation. We do so by examining first the limitations of existing techniques, and then, from this base, determining how best to evade existing geolocation techniques. We also consider two further geolocation techniques which may be of use even against adversarial targets: (1) the extraction of client IP addresses using functionality introduced in the 1.5 Java API, and (2) the collection of round-trip times using HTTP refreshes. These techniques illustrate that the seemingly straightforward technique of evading geolocation by relaying traffic through a proxy server (or network of proxy servers) is not as straightforward as many end-users might expect. We give a demonstration of this for users of the popular Tor anonymizing network.

1.6 Title: The Future Of Cybertravel: Legal Implications Of The Evasion Of Geolocation

This article analyzes the current legal status of cyber travel and explores how the law may treat cyber travel in the future. The analysis of the current legal framework covers copyright as well as other legal doctrines and the laws of multiple countries, with a special emphasis on U.S. law. The future of the legal status of cyber travel will be strongly affected by the desire of countries and many Internet actors to erect borders on the Internet to facilitate compliance with territorially-defined regulation and enjoy the advantages of a territorially-partitioned cyberspace. This article makes an attempt to identify arguments for making or keeping certain types of cyber travel legal and suggests legal, technological, and business solutions for any cyber travel that may be permitted.

Existing System

Client Presence Verification (CPV), a delay-based verification technique designed to verify an assertion about a device's presence inside a prescribed geographic region. CPV does not identify devices by their IP addresses. Rather, the device's location is corroborated in a novel way by leveraging geometric properties of triangles, which prevents an adversary from manipulating measured delays. To achieve high accuracy, CPV mitigates Internet path asymmetry using a novel method to deduce one-way application-layer delays to/from the client's participating device, and mines these delays for evidence supporting/refuting the asserted location. We evaluate CPV through detailed experiments on PlanetLab, exploring various factors that affect its efficacy, including the granularity of the verified location, and the verification time. Results highlight the potential of CPV for practical adoption.

3.1.1 DISAVANTAGES

- CPV rejects nearby and more distant intruders.
- One way delay can be affected by synchronization uncertainties.

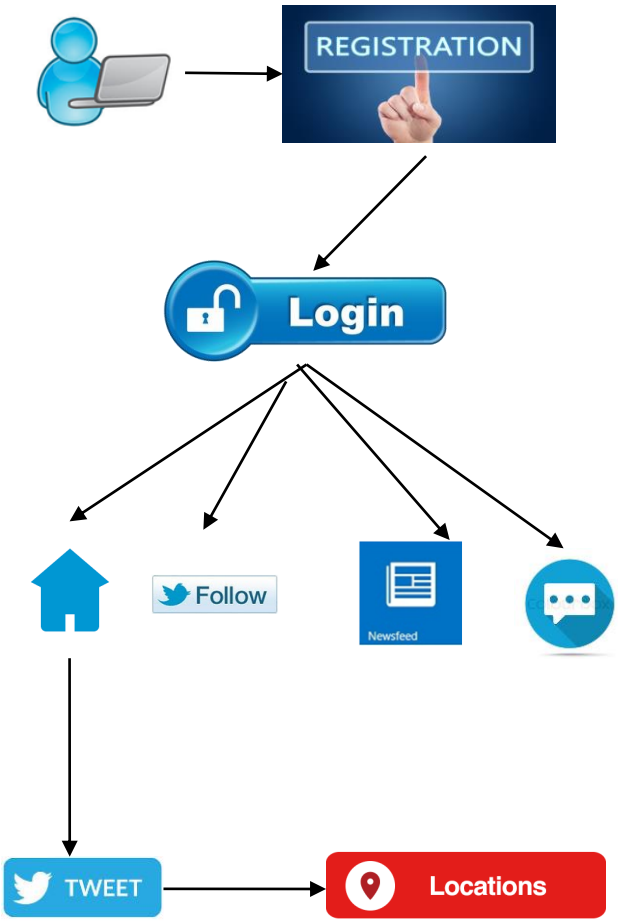
3.2 PROPOSED SYSTEM

A number of services in internet require the user's location. This is mainly done for some security purposes. Few internet services are in need of the user's geographical locations when they access these services. Intruders can easily escape the existing geo location techniques. This is done by faking the GPS co – ordinates or employing a dynamic IP address through proxy and VPNs. In this paper, a novel technique called User Location Identification (ULI) is introduced to verify a user's location prescribed in a geographic location. This technique doesn't identify the users by their IP addresses. HTML5 Geo location can be implemented if the user's device is a mobile device with GPS or GPS like triangulation features. This will give much more accurate information than the Geo – IP address. If the user's device does not use GPS it may alternatively influence the local SSID information and compare with other datasets to verify its physical location. This prevents an intruder from manipulating delays. ULI reduces the opportunity of intruders by implementing one –way application delay from or to the user's device and evaluates these delays as a proof for locating the user's location. This approach is implemented in social networks like Facebook, Twitter or Instagram and the various factors like efficiency, location, user's access time are evaluated. Experimental results show that ULI predicts the user's location in an effective manner.

3.2.1 ADVANTAGES

- Identifies the location of client exactly.
- The city's location is verified very quickly.

Architecture Diagram



CONCLUSION

The design of the proposed method provides several security and deployability advantages. This method requires no client-side changes and no extra software is needed. The client's current browsing experience is retained as the verification process runs in the browser. These advantages and the real-world evaluation results highlight this method's potential for practical adoption.

REFERENCES

[1] Shin et al., "Clock Synchronization for One-Way Delay Measurement: A Survey," in Advanced Communication and Networking. Springer, 2011, vol. 199, pp. 1–10.

[2] Shalunov et al., "A One-way Active Measurement Protocol (OWAMP)," RFC 4656, 2006.

[3] A. Vakili and J. Gregoire, "Accurate One-Way Delay Estimation: Limitations and Improvements," IEEE Trans. Instrum. Meas., vol. 61, no. 9, pp. 2428–2435, 2012.

[4] K. Claffy, Y. Hyun, K. Keys, M. Fomenkov, and D. Krioukov, "Internet mapping: From art to science," in Proc. IEEE CATCH, 2009, pp. 205–211.

[5] Y. Shavitt and E. Shir, "DIMES: Let the Internet measure itself," Comput. Commun. Rev., vol. 35, no. 5, pp. 71–74, 2005.

[6] M. Latapy, C. Magnien, and F. Ouédraogo, "A radar for the Internet," in Proc. IEEE Int. Conf. Data Mining Workshops, 2008, pp. 901–908.

[7] R. Landa, R. G. Clegg, J. T. Araujo, E. Mykoniati, D. Griffin, and M. Rio, "Measuring the Relationships between Internet Geography and RTT," in IEEE ICCCN, 2013.

[8] A. Pathak, H. Pucha, Y. Zhang, Y. C. Hu, and Z. M. Mao, "A measurement study of Internet delay asymmetry," in Springer PAM, 2008.

[9] A. M. Abdou, A. Matrawy, and P. C. van Oorschot, "Accurate One-Way Delay Estimation with Reduced Client-Trustworthiness," IEEE Commun. Lett., vol. 19, no. 5, pp. 735–738, 2015.

[10] I. Cunha, R. Teixeira, D. Veitch, and C. Diot, "DTRACK: A System to Predict and Track Internet Path Changes," IEEE/ACM Trans. Netw., vol. 22, no. 4, pp. 1025–1038, 2014.