Position Paper

Location Privacy in Next Generation Internet Architectures

Oliver Hanka
Technische Universität München
Institute of Communication Networks
80333 Munich, Germany
oliver.hanka@tum.de

Abstract

The locator/identifier–split concept is a much discussed and promising basis for a Next Generation Internet architecture. This addressing scheme solves several of the problematic issues of today's Internet. In terms of privacy, however, it introduces new tracking possibilities which need to be addressed. This position paper briefly discusses the location privacy problem of a locator/identifier–split architecture and outlines two possible solutions to it. Open topics, like lowering the negative impact of the solutions and calculating its additional costs for the network, are described.

1. Introduction

Much effort is put into developing a Next Generation Internet architecture to overcome the limitations of today's architecture. One aspect is to research novel addressing schemes to deal with scalability and mobility issues. While not being some sort of standard, many researchers agreed that the so called locator/identifier–split is a very promising approach. The locator/identifier–split provides two addresses for each node instead of a single one like today's IPv4 or IPv6 address. The two semantic meanings of the IPv4 address—*who* do I want to contact and *where* can I find him—are reflected by two independent addresses, the identifier and the locator. The identifier is assigned to a node for a long period of time and rarely or even never changes. All applications use the identifier to address a peer. In contrast, the locator reflects the topological point of attachment towards the network and is used to forward packets to a specific node. The locator is subject to change whenever a node roams. To be able to communicate, a mapping directory is required. This directory is an element within the network and informed of any locator change. Nodes can query the mapping directory to retrieve the current locator for any identifier. In which way such a mapping directive can be realized, is beyond the scope of this position paper.

2. Problem statement

While the locator/identifier–split principle has many advantages over today's IP architecture [1], it has one major drawback. By knowing an end–systems identifier, anyone is able to initiate a lookup in the mapping directory to find the whereabout of that node—and most likely also about the person owning it. Repeated over time, a movement profile is disclosed and can be used for either advertisement, legal prosecution or criminal means (see Figure 1). It is even possible to predict a node's future position based on historical data with a very high success rate [2].

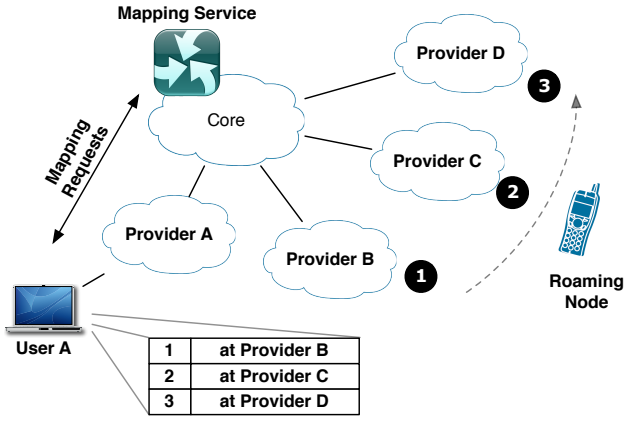

Figure 1. Movement profile through locator/identifier–split

It is, therefore, necessary to hide the routable address from other communication partners while still allowing them to contact the protected end–system. Not every system participating in the Internet, however, is subject to tracking. Non–mobile nodes, such as servers, or non–personalized nodes, like sensors, may not need the additional effort to protect their privacy. As any mechanism introduces overhead to the architecture, the goal should be to limit this to systems requiring the service instead of all network elements.

3. Possible solutions

The goal for a feasible solution should be to provide end–to–end connectivity while, at the same time, hiding the location of a node from its peers. This can be achieved by using proxies at the network layer—respectively a corresponding layer or building block in a Next Generation Internet architecture. A packet or stream would be addressed to the proxy which relays the packet to the correct destination. The end–to–end connectivity can be provided for all higher layers above the network layer. The proxy, however, must be aware of the current locator of a node. It must be able to resolve the mapping between the identifier and the *hidden* locator.

The use of a proxy in the communication path, however, has some disadvantages which need to be addressed and overcome. The first problem is the positioning of the proxy to minimize triangular routing. In case the proxy is not on the direct path between both end–systems, the connection experiences additional delay due to the suboptimal path it is routed. The second problem is the bottleneck of the proxy as many communication flows have to pass through it. An optimum between the number of required proxies and a feasible capacity utilization of a single machine needs to be found.

Gateway Solution. One possibility is to use gateways in the access network. An end–node sends all packets to the gateway only including the identifier in the header. The gateway is responsible for the address translation and queries the mapping system for the current locator. The benefit would be that only providers are aware of the locators. In that way it is similar to the Global System for Mobile Communications (GSM). A Mobile Station Roaming Number (MSRN) is assigned to each handset and the Home Location Register (HLR) is updated with the current valid MSRN. A phone call, however, is initiated by the Mobile Subscriber ISDN Number (MSISDN). The network itself has to query the HLR to map the MSISDN to the current valid MSRN [3].

Proxy Solution. Another approach is to place proxies [4] or forwarding agents [5], [6] somewhere within the network. End–nodes then have to resolve the mapping by themselves (e.g. query a mapping system). Nodes wanting to protect their privacy associate themselves with a privacy proxy provider and push the locator of the proxy or forwarding agent into the mapping system. The proxy receives any packet or stream destined to that node and forwards it to the real locator. By placing the proxies wisely within the network, the disadvantage of triangular routing can be lessened.

4. Current state / Future Work

The gateway solution approach has two disadvantages. The computational power of the end–nodes is not used for the mapping requests and must be provided by the edge network. This means increased costs for the providers. Furthermore, not all nodes require privacy protection (e.g. stationary nodes). The gateway solution, however, affects any communication. We, therefore, proposed a proxy based solution [4].

Currently we are researching ways to lessen the impact of triangular routing for the proxy solution. The idea behind this is to select a proxy which is closest to the communication path between two nodes. By integrating the proxy selection into the mapping system, the mapping system could select a proxy close to the requester. This of course would require global operating privacy proxy providers and increase the required computational power of the mapping system.

In a next step we want to determine the total costs of location privacy. Privacy does not come without a price tag, as any solution adds costs to the network. By investigating CAPEX, OPEX and customer inconvenience (e.g. delay, etc.) we want to compare different privacy approaches.

References

[1] B. Quoitin, L. Iannone, C. de Launois, and O. Bonaventure, "Evaluating the benefits of the locator/identifier separation," in *MobiArch '07: Proceedings of 2nd ACM/IEEE international workshop on Mobility in the evolving internet architecture*. New York, NY, USA: ACM, 2007, pp. 1–6.

[2] C. Song, Z. Qu, N. Blumm, and A.-L. Barabasi, "Limits of Predictability in Human Mobility," *Science*, vol. 327, no. 5968, pp. 1018–1021, 2010. [Online]. Available: http://www.sciencemag.org/cgi/content/abstract/327/5968/1018

[3] M. Mouly and M.-B. Pautet, *The GSM System for Mobile Communications*. Telecom Publishing, 1992, foreword By-Haug, Thomas.

[4] O. Hanka, "A Privacy Service for Locator/Identifier-Split Architectures Based on Mobile IP Mechanisms," in *Advances in Future Internet (AFIN), 2010 Second International Conference on*, Jul. 2010, pp. 6 –10.

[5] J. Ylitalo and P. Nikander, "BLIND: A Complete Identity Protection Framework for End-Points," in *Security Protocols*, ser. Lecture Notes in Computer Science, vol. 3957. Springer Berlin / Heidelberg, 2006, pp. 163–176.

[6] A. Matos, J. Santos, S. Sargento, R. Aguiar, J. a. Girão, and M. Liebsch, "HIP location privacy framework," in *MobiArch '06: Proceedings of first ACM/IEEE international workshop on Mobility in the evolving internet architecture*. New York, NY, USA: ACM, 2006, pp. 57–62.