DOER for Summer 2020 ILNP Project

170011568 - Max Evans

June 2020

1 Description

The aim of this project is to produce a research study concerning the security and privacy of ILNP - a network-level protocol designed to be an "evolutionary enhancement" to IP, the internet architecture's current method of addressing. The title of study will be "Comparing IPv6 Security and Privacy with ILNPv6".

The paper will focus on the fundamentals of network design and how the current internet architecture implements these ideas - this will occupy a section detailing underlying networking concepts, and will be included to introduce security and privacy concerns inherent to complex networking systems, as well as giving a fairly comprehensive overview of the motivation for ILNP in general (i.e. applications in multihoming and the "semantic overload" of the IP address). This will hopefully be in an effort to reveal that security/privacy as a part of the internet system under IP has been included as an afterthought rather than a consistent element ingrained into its design.

The study will investigate the purported ways ILNP incorporates security and privacy into its design, and why the generic design approach of "secure by design" benefits the internet architecture in contrast to the mechanisms that have been built using strictly IP.

2 Objectives

The ultimate deliverable of the study is the singular research paper which should aim to achieve three things:

- To critically compare the ways that ILNP provides location and identity privacy to that which is not achieved via IPv6
- To evaluate the changes that would have to be made to ILNPv6 such that ILNP functions with the IPSec protocol suite
- To critically evaluate and compare the mechanisms ILNP provides to achieve NAT, Multihoming, and (one other thing) in aim to help identify weaknesses in ILNPv6 *and* IPv6

The final deliverable is described as a study, and, unfortunately, due to the current pandemic and various other factors, should not contain experimental or practical work (systems or coding) done in the lab environment at St. Andrews University.

Concerning the first of these objectives: location privacy concerns a protocol's support for masking the physical location of a node. From an objective privacy standpoint, deep packet inspection measures used to reveal IP addresses may allow malicious endpoints, organisations, or states, to discover, albeit to varying degrees of accuracy, the location of a node - ILNP is said to include mechanisms which ensure location privacy, these measures will be studied and reported in depth, however, as mentioned, not much can be done to test this functionality.

The second part of the first objective scrutinises ILNP's ability to provide mechanisms that ensure a node's identity privacy. The motivation for this feature comes, again, from ways that the IP architecture fails to provide identity privacy to users. Identity privacy concerns a protocol's ability to mask the user of a network node, i.e. the fact of being what or who a person is. IP addresses on their own do not jeopardise identity privacy like they do with location privacy, however, a system administrator to a website or other service does have the ability to maintain the IPs of the users to their site - this allows them to congregate impressions left by users that may jeopardise their identity to be tracked alongside the single IP address they use to communicate with the service.

As a part of the current internet architecture, measures that have been taken to ensure these privacy concerns "on top of" the current internet architecture do not necessarily solve the problem of location or identity privacy. A common approach is that of Virtual Private Networks (VPNs), who ensure location and identity privacy by allowing subscribing users to occupy endpoints in differing locations to their own, and host many server endpoints with altering IPs that users may switch to at any moment. A popular scrutiny of VPN providers is that they simply provide a shallow facade of identity and privacy mechanisms, and do not solve the actual problem. This is because they still occupy a body with access to their users' actual IP addresses, and may use the methods discussed here to determine their user's identity and location. This is mentioned as it exemplifies the extent that individuals must go to in order to ensure privacy - it is hoped that ILNP provides a more fundamental approach to solving these problems such that nodes may privately communicate without the need for complex, external mechanisms that come with their own drawbacks.

The second of the objectives concerns detailing the changes that would need to be made to ILNPv6 in order to ensure its compatibility with IPSec. IPSec is a protocol suite that looks to generate and maintain an encrypted channel between devices. ILNP's current functionality preventing its interoperability with IPSec will be examined at length a potential solution will follow.

The last objective concerns an aspect that should be present throughout the study - the critical comparison of ILNPv6 and IPv6, the namesake of the paper. However, to highlight the fundamental differences in the protocols, and to gain a better architectural understanding on how both protocols intent to function with the current internet, the mechanisms of NAT, Multihoming and TBA will be discussed at length in terms of how each protocol achieves them.

3 Ethics

This study does not require the handling or use of sensitive data, nor does it concern working or experimentation with human subjects (not even myself), only the information they have already freely provided as a result of previous research, which will be cited and properly accredited as per the expectation of any academic work.

4 Resources

As per my initial research, much of what is needed for a study of this scope can be gathered through open source research performed by academics at the University of St. Andrews and other institutions. Resources specifically available through the IEEE website can be easily accessed through a Shibboleth identity provider that I can use with my University login. The project, alongside any accompanying documents will be version controlled through the University's GitLab host - which does require a consistent access to the lab environment via SSH (and SOCKS for browser viewing).