# Protective Internet Protocol (PIP)

Zhenhua Liu[*], *Student Member, IEEE*, Xiaoping Zhang[†] , Lars Westberg[‡] , Youjian Zhao[†] , Ling Chen[‡]
[*]Graduate Student, Dept. CS&T, Tsinghua University, Beijing, China, zhenhualiu@ieee.org
[†] Faculty, Dept. CS&T, Tsinghua University, Beijing, China, {zhxp, zhaoyj}@tsinghua.edu.cn
[‡] Researcher, Ericsson, Sweden, {lars.westberg, ling.chen}@ericsson.com

## ABSTRACT

In this paper, we show how a network layer provides *protection*, the ability to prevent attacks from happening *ex ante*. We present the basic design of the Protective Internet Protocol (PIP), an architecture supporting protection and discuss future directions.

## I. INTRODUCTION

Security is becoming the first concern of the Internet. In particular, the IP network layer provides little, if any, *reachability* control against attacks. The location information is open to anyone, which means any host can send packets to any other hosts without permission of receivers. This is also the fundamental vulnerability for attacks such as Denial of Service (DoS) attacks. Proposed approaches can be classified into two categories: reactive, e.g. [1], and proactive, e.g. [2].

In this early paper, we investigate the feasibility of protecting location information through address space and present the basic design of the Protective Internet Protocol (PIP), a network architecture that provides protection against location information leakage. PIP uses *tags*, instead of IP addresses, to make the protection of location information possible.

The major contributions of the paper are as follows. First, we analyze the problem of information leakage under current IP architecture and initiate our study of PIP based on this principle. To the best of our knowledge, this is the first time to use information theory, especially entropy, to provide a quantitive analysis. Second, we present the basis design of PIP. This architecture focuses on reachability and protects the location information through transformations of address space. Furthermore, we develop Tag-based Forwarding (TF) to realize PIP. We formulate the problem and find out that all solutions form a permutation group. This result characterizes the nature of PIP. Last but not least, we provide the practical considerations.

We do not claim PIP is sufficient or optimal and we agree that the general problem of control over host reachability is a non-trivial one [2]. In this paper, our primary goal is to exploring how to protect location information solely through operations on address space, which provides a new direction for future research.

## II. LOCATION INFORMATION LEAKAGE

Under current architecture, when a (source) host sends a request to the DNS for the IP address of a certain domain name, DNS will reply with neither limitations nor control. Based on information theory, we can use entropy to describe the extent of uncertainty of an event. Formally, let $A=\{A_1, A_2,\ldots, A_n\}$, where the probability of $A_i$ is $p_i$, , and $p_1+p_2+\ldots+p_n=1$. Then the entropy of $A$ is:

$$H(A) = -p_1 \log p_1 - p_2 \log p_2 - \cdots - p_n \log p_n$$

For IPv4, a host without the knowledge of the corresponding IP address for a certain domain name will consider every possible IP address with equal possibility. So the entropy is (roughly) 32bits. After it obtains the reply from DNS, the entropy is 0. In other words, DNS sends the entire location information to hosts.

Since most attacks are launched by malicious hosts, we are motivated to ask: do we really have to send location information that can be utilized by attackers to hosts? The answer is no, especially from the security's point of view.

Fig. 1 depicts model of location information transfer. In this model, we abstract the Internet into three parts: DNS, router system and host system. DNS has full information and host system requests DNS for the match of IP addresses and domain names. The information transferred from DNS to host system is $H_1$. When host sends packets to router system, it sends information $H_2$ to router system in order to perform a correct forwarding. DNS will send information $H_3$ to router system, if necessary. For IPv4, $H_1 = H_2 = 32$ bits and $H_3 = 0$.

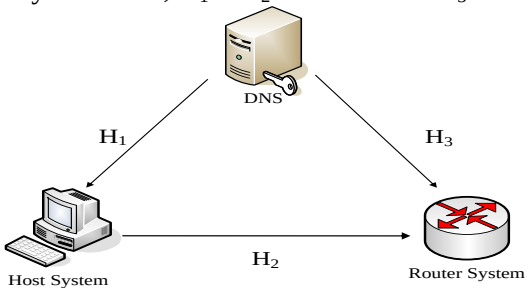


Fig.1. Location information leakage.

## III. THE PIP ARCHITECTURE

Under PIP, IP addresses are replaced by *tags*, which can be regarded as a generalization of IP addresses. Every host has its own Identity Name (IN), just like domain name under current architecture. With INs and tags, we

can separate identifiers and locators solely in the network layer, similar to [3]. In PIP, when a (source) host requests DNS for the destination tag of an IN, he has to send his own tag and DNS will perform reachability control. If the source is qualified, DNS will reply with the destination tag and source host can use this tag to send packets to the destination, which means once the host obtains the tag, he will behave exactly as that under current IP architecture.

However, tags are essentially different from IP addresses in the following aspects. First, IP addresses contain both identity and location information, but tags contain only location information, which makes protection of location information *possible*. Furthermore, when replying with tags, DNS will check the tag of the source host to ensure the host is allowed to send packets to the destination. Note that we do not limit the reachability control to any particular policy, so PIP can support different demands. The tag verification is similar to that in Section 3.1 of [1]. Finally, tags are changed when necessary according to the deployed policy, which means tags can have TTL (Time To Live) if necessary. This makes protection of location information *feasible*.

In order to perform packet forwarding correctly, routers have to know the topology information and the location information of the destination. The former one is matching every IN to a particular next-hop (out-port) and the latter one is matching every destination tag to a particular IN. Combining both we can map every tag to a particular out-port, and these mappings form the routing table. With this routing table, routers can forward packets properly. In PIP, the topology information is still obtained through routing protocols such as OSPF and BGP. However, the matching of INs and tags is sent from DNS directly to routers, without the relay by hosts.

## IV. TAG GENERATION

As shown in Fig. 2, tags can be generated by every IP address (a) or every subnet (b). The first column in both figures is the IP address space, which is divided into continuous subnets, each corresponding to a route entry. The second column is the tag space, which can be done by tag generation.

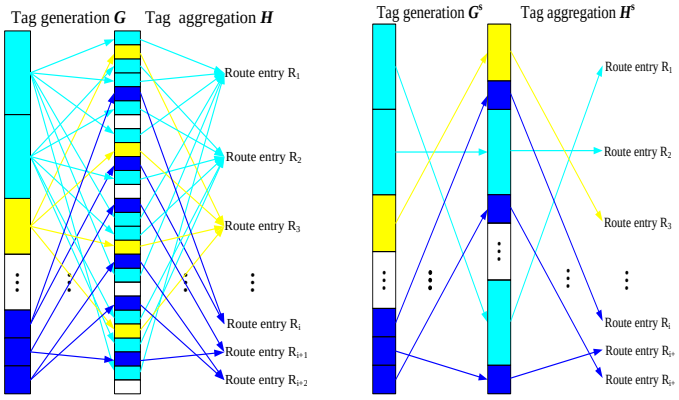


Fig.2. Tag Generation: (a) IP-based; (b) Subnet-based.

Tag generation can be considered as a permutation of IP addresses/subnets. Permutation group is defined as the group of all the permutation of a non-empty, finite set ***A***. If we treat every address/subnet as an element in ***A***, then all the tag generations form the permutation group of set ***A***. If ***A*** contains *n* elements, then there are *n*! different permutations. This is complex enough for the security requirement. We can also encrypt IP addresses to obtain tags, which is the identical permutation. In PIP, we favor subnet-based tag because it achieves satisfactory security while keeping route aggregation of current architecture.

## V. PRACTICAL CONSIDERATIONS

Routers cannot rely on current TCAM scheme to deal with subnet-tag. So we consider the following possible solutions. We can use special hardware to perform the routing lookup, where we use both the upper bound and lower bound of each subnet as the route entry. Also we can use two-step lookup: first translate tags to corresponding INs, then use these INs for routing lookup.

PIP can realize incremental deployment, which is essential for the real deployment of secure mechanism. According to the proportion of the Internet supporting PIP, there are three stages: separate-subnet stage (initial stage), overlay stage (transition stage) and Internet stage (final stage).

## VI. CONCLUSION AND FUTURE DIRECTION

It is high time that Internet performs reachability control to provide protection against attacks. No longer should the location information be open to the attackers, nor should attacker be able to launch attacks without limitation. By generalizing IP addresses to tags, we introduce Protective Internet Protocol architecture with Tag-based Forwarding, an entirely new architecture providing protection of location information.

This work is in its early stage and we list several further directions. First, the impact of this architecture on the routing infrastructure is not clear and we are planning more simulation and performance measurement. Also, in PIP, DNS plays a vital role, which makes the DNS's security situation even worse. All the schemes aiming at improving the security of DNS will contribute to PIP. Finally, we want to know how well can PIP provide protection from externally generated DoS-attacks.

## REFERENCE


[1] D. Andersen, H. Balakrishnan, N. Feamster, T. Koponen, D. Moon and S. Shenker. Accountable Internet Protocol (AIP). *In ACM SIGCOMM 2008.*

[2] H. Ballani, Y. Chawathe, S. Ratnasamy, T. Roscoe, and S. Shenker. Off By Default. *In HotNets-IV*, 2005.

[3] R. Moskowitz and P. Nikander. Host Identity Protocol (HIP) Architecture. *RFC 4423*, 2006.