Umbrella: A Routing Choice Feedback Based Distributed Inter-Domain Anti-Spoofing Solution

Jie Li[*,2], Jun Bi [†,1], Jianping Wu [‡,1,2]
[1] Network Research Center, Tsinghua University, Beijing, China
[2] Dept. Computer Science & Technology,Tsinghua University, Beijing, China
[*] jieli@csnet1.cs.tsinghua.edu.cn, [†] junbi@tsinghua.edu.cn, [‡] jianping@cernet.edu.cn

***Abstract*—The authentication of the IP source address remains one of the most important steps in making the Internet as trustworthy as possible. With existing anti-spoofing solutions, deployed ASes lack cooperation when exchanging routing decisions and disseminations. In general, this makes anti-spoofing mechanisms inefficient and does not adapt to incremental deployment. By introducing routing choice feedback, we propose a distributed inter-domain anti-spoofing solution (Umbrella). In Umbrella, the deployed ASes can acquire approximate global routing choice information. Our approach offers gains in efficiency through the verification of the packets forwarding path and the construction of dynamically spoofing packets filter. Our experimental analysis of Umbrella shows it to be both effective and incrementally deployable.**

I. INTRODUCTION

The Internet's architecture includes no explicit notion of packet-level authenticity. This functional deficiency enables attackers to easily spoof IP source addresses. By masquerading as a different source, an attacker can stage attacks that undermine the security of fundamental Internet applications and redirect blame, and even induce millions of dollars of financial losses, such as DoS/DDoS, Botnets, Spam, TCP hijacking, DNS poisoning, etc [1]. Moreover, due to the difficulty of pinpointing the true origin of an attacker, IP source address spoofing is still a common and popular attack vector.

Although attackers can insert bogus source addresses into IP packets, they cannot control the actual paths that the packets take to the destination. Using path authentication, therefore, is a clever way of defeating spoofing attacks.

In this paper, we propose a distributed inter-domain anti-spoofing solution, called Umbrella. By means of inter-domain routing system cooperation, Umbrella utilizes a novel route-based packet filter as a way to mitigate IP spoofing. Umbrella addresses inter-domain routing system cooperation by addressing the implications that AS border routers (ASBR) can authenticate the source of a packet and filter spoofed packets at high-speeds based on the routing choice feedback within the Trust Alliance (Section II-A). The routing choice feedback can help to build a more specific and accurate route-based packet filtering table. Thus, Umbrella offers desirable benefits and incentives: 1) Knowledgeability: Umbrella makes control plane of ASBR knowledgeable by employing the Routing Choice Feedback message (RCF), which makes the inter-domain routing system cooperation feasible and easy to acquire approximate global routing choice information within TA; 2) Scalability: Umbrella enhances the ability of ASBR by enabling the data plane to checking source address without any modification to the de facto packet structure; 3) Security: Under the assurance of inter-domain routing system cooperation, Umbrella has the effect of facilitating the process of verifying accurately the packets forwarding path and constructing dynamically bogus packet. Thus, Umbrella also establishes and maintains a *deploy early and benefit rapidly* incremental deployment incentive mechanism.

This work was supported by National Science Foundation of China under Grant 61073172, Program for New Century Excellent Talents in University, Specialized Research Fund for the Doctoral Program of Higher Education of China under Grant 20090002110026, and National Basic Research Program ("973" Program) of China under Grant 2009CB320501.

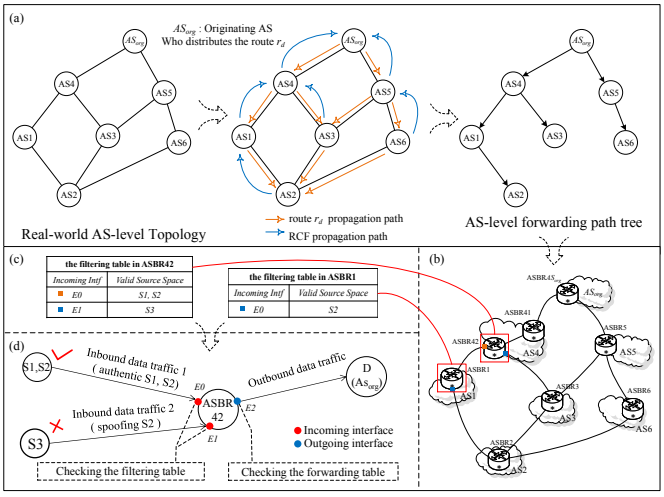

Fig.1. A RCF-based distributed inter-domain anti-spoofing solution (Umbrella)

II. DESIGN PRINCIPLE OF UMBRELLA

A. Basic Definition

We introduce a BGP extension based on employing a new BGP message, named Routing Choice Feedback (RCF). RCF's BGP Path attribute is set to optional transitive, which provides a backward compatibility for legacy ASes. All Umbrella-enabled ASes (hereinafter as AS for brevity) consist of a Trust Alliance (TA), i.e. a multi-AS trustworthy networks. All ASes cooperate on consulting the routing choice information by exchanging RCF.

1. The Methodology of Generating Filtering Rules

In Umbrella, each ASBR uses BGP routing updates and a set of local preference rules to calculate a best forwarding path and determine the outgoing interface for each destination address space. RCF messages are designed to inform ASBRs about the path that has already been chosen by downstream ASes, thus allowing all ASBRs on the path to a destination to deduce valid incoming interfaces for specific source address spaces.

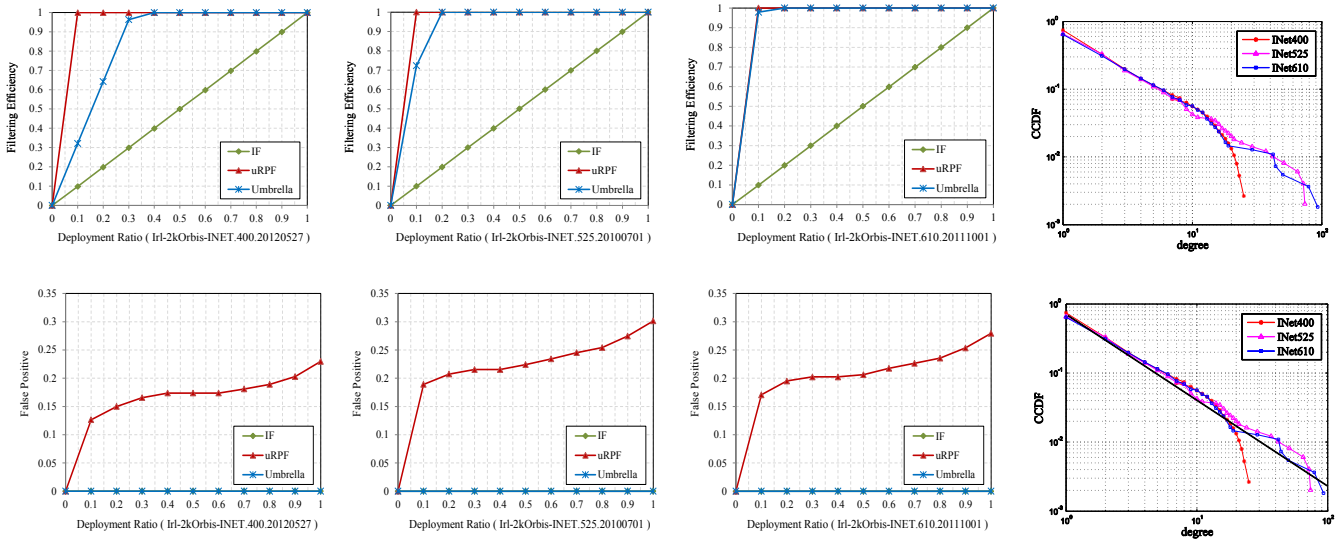

Fig. 2. The Experimental Evaluation of Umbrella

Fig. 3. The CCDF

2. Generating the AS-level Forwarding Path Tree

Upon receipt of the route r_d, each ASBR residing in a downstream AS node adopts the r_d as the route heading toward a certain destination prefix p_d. The RCF is then forwarded along the reverse path to the upstream neighbor AS, that advertised the r_d. In this fashion, each AS forwards its RCF backtrack to its upstream neighbor hop by hop, until the RCF reaches the originating AS AS_{org}. Finally, AS_{org} can build a logical AS_{org}-root directed AS-level forwarding path tree. Within this tree, each AS node represents a specific source address space and is associated with a specific incoming interface. Fig.1(a) shows an example of this process. Triggered by both routing changes and forwarding table changes, Umbrella uses a scheme of sending RCF message to reconstruct eventually the logical AS_{org}-root directed AS-level forwarding path tree.

3. Generating the RCF-based Filtering Table

Each ASBR residing in an AS on the AS-level forwarding path tree uses the received RCF to maintain its AS-level forwarding path tree. Thus each ASBR can record the path that the RCF has traversed before reaching it and ensure that the RCF follows the same path toward the specified destination address space the same way as valid data packets do. Finally, the RCF is further processed to help ASBR build a route-based filtering table as to source address spaces mapping to incoming interface (Fig.1(b,c)) in a distributed fashion. If an AS node's parent is changed, the AS node's new parent will automatically modify its incoming interfaces so as to remap all descendant source address spaces are related incoming interfaces on AS-level forwarding path tree. This change will be updated automatically to the parent's filtering table.

B. Processing the Routing Choice Feedback Message

Each AS node not only forwards its own RCF message but also piggybacks other downstream AS nodes' RCF messages backtrack to the originating AS AS_{org} hop by hop. In order to reduce bandwidth consumption, we enable aggregation in RCF. We set a timer to enable an efficient piggyback and then RCFs can aggregate along the route as much as possible.

C. The Implementation of the RCF-based Spoofing Filtering

The intuition in Umbrella is that, assuming single-path routing at a given time period, there is exactly one single valid *path<s,d>* between source node *s* and destination node *d*. Hence, any packets with source address *s* and destination address *d* that appear in a ASBR not in *path<s,d>* should be discarded. Umbrella uses a routing choice feedback based filtering table to determine if a packet arriving at an ASBR is valid with respect to its inscribed source-destination address pair and then identifies and discards forged IP flows. (Fig.1(d)).

III. EXPERIMENTAL EVALUATION

To evaluate Umbrella, we simulate 3 group AS-level experiment topologies: {*N* (# of AS) =400},{*N*=525},{*N*=610} and focus on two key evaluation indicators: filtering efficiency and false positives. Experimental results show that Umbrella is effective and superior to the other filtering methods (Ingress Filtering and uRPF) without introducing any false positives, especially in a typical power-law AS-level topology (Fig.2.3).

IV. CONCLUSION

Our proposed protocol, Umbrella, is adept at flexibly enabling inter-domain routing system cooperation by making use of a routing choice feedback mechanism. The use of this architectural enhancement offers a way to facilitate Umbrella to be effective, backward compatible and incrementally deployable. In the future, we will further study how an AS can acquire or speculate the details of neighbors' routing information and business relationships by exchanging additional information.

REFERENCES

[1] Network Infrastructure Security Report, Arbor Networks. Feb., 2011.

[2] T. Ehrenkranz and J. Li, "On the state of IP spoofing defense," ACM Transactions on Internet Technology, vol. 9, no. 2, 2009.

[3] R. Beverly, A. Berger, Y. Hyun, and K claffy. Understanding the efficacy of deployed internet source address validation filtering. In IMC, 2009.