CS4516: Project Intro and Conclusion

Tag-Based IP Spoofing Prevention Under Low Deployment Scenarios

Author:
Michael Calder
Daniel Robertson

Supervisor:
Dr. Craig Shue

March 2, 2014

1 Introduction

A critical vulnerability exists within the very threading of the Internet. Our world's backbone for digital information exchange focuses naively on the receiver of a transmission, without giving proper regards to who the sender is. Malicious attackers exploit this short sight in order to temporarily disable target servers by issuing more requests then the target can handle, a technique known as denial of service (Dos). An attacker who rapidly alters, or spoofs, the source IP address on traffic they generate cannot be tracked. Existing counter measures attempt to mitigate the effect of DoS attacks on the server, but fail to address the underlying issue at hand.

1.1 Background and Motivation

Shue et. al propose an eloquent solution which effectively curbs IP spoofing at the source. In their approach, implementing routers inspect the source address of each packet, and ensure that it is a conforming address with respect to their subnet [?]. Explicitly, if this router's subnet was 130.215.0.0/16 (that of the university this research was conducted under), and an encountered outgoing packet had a source IP of 176.230.1.5, the packet would be dropped. Should inspection pass, a unique tag (known by each other implementing router) which identifies the particular router, is added to the packet. Each downstream router en route to the destination checks for the presence of such a tag, and adds its own if one is found. Their analysis proves that their protocol is able to deny spoofed IP packets from entering the larger network at a rate nearing 100%. The catch, however, is that this effectiveness is contingent on a high deployment status

Shue et. al note that the integrity of a given packet tag is weak under topologies with partial protocol deployment. A compromised tag threatens to undermine the efforts of the IP Spoofing prevention. Their own analysis shows that when only 10% of the network implements their anti-spoofing protocol, then 66% of networks can abuse a leaked tag (assuming 100% collusion) [?][1]. As the cost of changing router functionality to implement the protocol is likely to deter deployment speeds, the problem of tag theft may discourage adoption.

[1] Under more realistic levels of collusion (10%), only 7% of stolen tags can be reused effectively

In an effort to smooth out the tag security concerns which emerge under low deployment scenarios, we propose two methods to secure the underlying packet tag implementation. Both combine a fast non-cryptographic hash algorithm (xxHash) with a nonce derived from the current unix time. By mending tag security concerns under low deployment, our modifications add further incentive to early adoption.

1.2 Related Work

Many approaches to preventing inter-domain IP spoofing (where attackers attempt to spoof IP addresses outside of their personal domain), already exist. Most prominent are those which attempt to trace the route of the attacking packet back to the (true) source, such as [?]. Shue et. al's approach follows more along the lines of packet filtering, ie. dropping packets near or around the source. Research such as [?] perform ingress filtering, which drop spoofed packets from within the originating network, but fail to cover packets that escape into the wild.