Denial of Services & Counter Measurements

Janneth Malibago <jannethm@student.ethz.ch>
Seminar of Distributed Computing WS 04/05

1 Summary

The original Internet architecture was designed to provide unicast point-to-point communication between fixed locations. In this basic service, the sending host knows the IP address of the receiver and the job of IP routing and forwarding is simply to deliver packets to the (fixed) location of the desired IP address. But, nowadays the Internet is available from everywhere by using any kind of device. Above all, the user is not restricted to a fixed location anymore. Thus, many applications would benefit from more general communication abstractions, such as multicast, anycast, and host mobility. But implementing these more general abstractions at the IP layer brings up difficult technical problems and major deployment barriers. All attempts to implement these more general abstractions have relied on a layer of indirection that decouples the sending hosts from the receiving hosts. But although several proposals achieve the desired functionality, they do so in a very disjointed fashion in that solutions for one service are not solutions for other services.

With the Internet Indirection Infrastructure (i3) the first paper [1] proposes a general overlay service that avoids both the technical and deployment challenges inherent in IP-layer solutions and the redundancy and lack of synergy in more traditional application-layer approaches. It combines the generality of IP-layer solutions with the deployability of overlay solutions. The main idea is to decouple the act of sending from the act of receiving. This is achieved by introducing an indirection abstraction: sources send packets to a logical identifier and receivers express interest in packets by inserting a trigger into the network. With this simple trick i3 can provide a general-purpose indirection service through a single overlay infrastructure. Further details on i3 can be found in [1].

But i3 does not only provide communication abstractions such as multicast, anycast or service composition but also enables other useful applications based on the Internet Indirection Infrastructure. For example in the second paper [2] the authors present how end hosts can defend themselves against denial-of-service attacks. Their main thesis is that end host and not the network should be given control how the packets which are addressed to the host should be processed. Using an i3-based approached gives a general and architecturally clean solution. The authors also point out how complicated an IP-based approach would be in contrary to an i3-based approach.

2 Analysis

i3 in its current state has several limitations. Not only are the details of the design still preliminary, but also the robustness of the approach still needs to be verified. And one should not forget to scrutinise the security of the system. The authors ran some simulations on a prototype and the results were promising. However, more applications need to be tested on top of i3 to ascertain its performance.

In my opinion the Internet Indirection Infrastructure is an interesting new approach which gives good ideas to solve several problems. Using an indirection abstraction seems to be the right way to find a solution which is general and yet simple. The problem is that the generality of i3, however, comes at the cost of security. I3 is more vulnerable to malicious attacks than the Internet as i3's flexibility is both a feature and a potential for abuse.

[2] discusses several counter measurements against packet flooding, but the approach is based on many assumptions and neglects many security issues. Furthermore the proposed solution actually does not really solve the denial of service problem. The proposed defences protect the end host, but what about the network itself?

The challenge is to design an indirection layer which is itself robust to denial-of-service attacks. An IP-based solution would not be general enough. On the other hand, an i3-based approach is not yet deployable. Furthermore the question remains if i3 can be as secure as the Internet. Of course the goal is to provide security without sacrificing flexibility. [4] shows how i3 can be flexible without compromising security and performance by introducing a re-design of the Internet Indirection Infrastructure which is called Secure-i3. Secure-i3 eliminates some vulnerabilities of i3 without sacrificing functionality. Details on Secure-i3 can be found in [4]. While in this paper, the authors have tried to argue that their system does not introduce new vulnerabilities, more remains to be done. As in [1] and [2] there are still several open questions.

Actually this point is common in all the papers mentioned. Several good ideas and approaches are proposed but there are as many questions that remain open. One could be annoyed by this fact but the authors do not hide that the results are still preliminary and the research is still going on (see [3]). I think the research around i3 is very promising. Maybe i3 is not the answer to the problem of denial-of-service attacks, but one day or another it will provide some new communication solutions.

References

[1] Internet Indirection Infrastructure
I.Stoica, D. Adkins, S. Zhuang, S. Shenker, S. Surana; SIGCOMM 2002

[2] Taming IP Packet Flooding Attacks
Daniel Adkins, Karthik Lakshminarayanan, Adrian Perrig, Ion Stoica (UC Berkeley and CMU); HotNets 2003

[3] http://i3.cs.berkeley.edu/

[4] Towards a More Functional and Secure Network Infrastructure
Daniel Adkins, Karthik Lakshminarayanan, Adrian Perrig, Ion Stoica; UCB Technical Report No. UCB/CSD-03-1242, 2003