Review of *Internet Indirection Infrastructure*

Matthew Renzelmann

March 22, 2007

1 Key Insights and Contributions

The primary contribution of this paper rests with its position that mobility, multicast, and anycast are difficult to deploy in the existing Internet. Rather than address each of these potential applications individually, the paper seeks to unify their implementation using *i3*. Like the approaches used to address many systems problems, *i3*'s solution involves adding a layer of indirection. Rather than route packets individually from a source to a destination, packets first travel from the source to an intermediate node which hosts a receiver's trigger. From there, the packet travels to the receiver (or receivers). Any node interested in receiving packets destined for specific identifiers simply create an appropriate trigger, or (identifier, address) pair. The authors also propose a number of extensions to enable more sophisticated functionality, such as stacks of triggers, and go on to conduct a preliminary performance review of the system.

2 Areas for Improvement

Unfortunately, *i3* opens up a variety of new avenues for malicious behavior. Publications subsequent to this one identify a wide array of security problems with *i3*. In addition to the problems discussed here, including eavesdropping, impersonation, and DoS attacks, *i3* also enables the following problematic scenarios:

- An attacker could inject a series of triggers that form a loop, so that data forwarded to any one of the triggers would cycle and waste resources.
- Similarly, instead of a cycle, the attacker could simply create a chain of triggers that terminates with an invalid host. Data sent to any trigger in this chain would be dutifully forwarded, only to be dropped at one end.
- Some of the security solutions described, e.g. requiring a challenge/response whenever a trigger is added, are vulnerable to man-in-the-middle attacks.

Fortunately, many of these issues should be addressable, or, in the worst case, are no more troublesome than in IP itself.

3 Implications for the Future

One question the authors did not address clearly was how *i3* might be deployed. In order for the system to make a meaningful impact on the future of the Internet, it might prove helpful to have some understanding of how ISPs might go about setting it up. *i3* clearly holds an advantage in that it ISPs can deploy it incrementally, but it is far from clear how they might make money off it, and whether potential customers would willingly pay for its functionality. In its present implementation, for example, there's no clear way to limit an individual from setting up a multicast to millions of people, which may upset their ISP.

Nevertheless, *i3* promises a great deal of flexibility and would substantially simplify or overcome many of the issues facing the Internet today.