# *Towards a More Secure and Robust Internet*

Pioneering Technologies
for a Better Internet

Cs3, Inc.

5777 W. Century Blvd.
Suite 1185
Los Angeles, CA 90045-5600

Phone: 310-337-3013
Fax: 310-337-3012
Email: info@cs3-inc.com

**Cs3 Inc.** Los Angeles, California

## Abstract

Using funding from the Defense Advanced Research Projects Agency (DARPA) and the California Technology Investment Partnership (CALTIP), Cs3 has taken up the challenge of constructing the building blocks for a more secure and robust Internet. The technology being built solves long-standing problems like elimination of IP source address forgery and paves the way for defenses against packet flooding and associated denial of service attacks. Key parts of these technologies are patent-pending. Implementation and testing of this technology is under way for both IPv4 and IPv6.

## Contents

## 1. Infrastructure Vulnerabilities and Their Impact

The Internet was designed for speed and growth. The infrastructure is certainly working as envisioned by that yardstick. However, the Internet continues to be vulnerable to different security and robustness problems. This paper focuses on some fundamental deficiencies in the Internet architecture and protocols, and ways to remedy these shortcomings. Emphasis is placed upon *infrastructure-level* issues rather than *site-level* problems such as virus protection, intrusion detection, password protection, etc.

Denial of Service (DoS) and Distributed DoS (DDoS) attacks are a prime symptom of underlying infrastructure deficiencies. In February 2000, coordinated attacks lasting just a few hours on EBay, Cnn, and Yahoo are estimated to have caused over $1 Billion in damages *[ Yankee Group ]*. Another attack in January 2001 on Microsoft is still being assessed for damage, but did great harm to the company's reputation. The Computer Emergency Response Team (CERT) warns repeatedly that there is currently no technology to deal with this problem and recommends general vigilance and administrative measures to minimize the potentially devastating impact of a DDoS attack.

Responding to the above and other kinds of security problems on the Internet is complicated by the fact that a packet's origin or source can be forged by those wanting to cause mischief and escape detection. A major weakness in the Internet protocols is that it is possible for packet source forgery to occur.

Some problems of "the Internet" are caused by bugs in the programs that implement its protocols. These bugs are, needless to say, exploited to do great damage. Recent furors over inadequacies in implementations of TCP and Domain Name Servers are examples of problems that will eventually be solved by removing the bugs from those implementations. The focus of this paper is on the inadequacies of the Internet protocols *as specified*, not the particular deficiencies of particular flawed implementations of the specification.

## 2. Existing Solutions

At present there is no deployed and fully automated solution to combat problems like source forgery or denial of service attacks. Traditional network security products, such as firewalls and intrusion detection systems, are not equipped to address infrastructure-level problems like these. Various manual procedures and processes are used to combat these problems:

- CERT Advisories [1] specifically about DDoS attacks. CERT suggests that every installation should protect its own machines to prevent them from being used as "slaves" in mounting attacks on third parties.

- WWW Security FAQ [2] Securing Against Denial of Service Attacks

- Cisco's recommended measures  [3] (both forensics and preventive) in reaction to DDoS attacks

- ISPs are advised to implement *ingress filtering* [4] which is supposed to filter exiting packets that do not have source addresses within its purview. This can reduce the packet source forgery problem. However, few ISPs do this because there is no direct benefit to their subscribers.

While the above measures are certainly useful to some small degree they do not constitute practical, reliable solutions to these important problems.

Finally, a number of recent startup companies have advocated an approach to the DDoS problem that we refer to as "Smart Filtering". These companies recognize that it is too late to solve the problem when the packets arrive at their destination. While we are not familiar with all the details of these proprietary approaches (because they have not been published), it seems that these approaches work through intelligent, rule-based analysis of patterns and rates of the traffic flowing through ISPs or at points even further upstream. The problem is that this approach can, at best, only recognize attacks that have been seen and analyzed before. The result is likely to be similar to what we see today in virus scanning software. The defenses are always trying to keep up with (and always fall a little behind) the attackers. Further, any analysis that makes use of the contents of packets is likely to fail as encryption becomes more widespread.

## 3. Cs3's Proposed Solution

In today's Internet, security and robustness are NOT simply properties of a single site. A site that requires communication over the Internet can be no more safe or reliable than the *public infrastructure* upon which it depends for critical functions. True, CIOs can only control their own sites, but increasingly they are suffering the devastating consequences of being connected to a vulnerable infrastructure.

The central premise motivating this company is that it is possible to build key mission-critical characteristics (e.g., security and reliability) into the public infrastructure so that *everyone* can derive the benefits of security and reliability without adversely affecting performance, and without compromising the essential nature of the Internet as an open, decentralized, affordable, and universally available utility. In particular, Cs3 focuses attention where it belongs: on the fundamentals of the Internet infrastructure itself. There are several important initial thrusts in the Cs3 technological approach to upgrading the Internet's reliability as a whole:

- **Elimination of Source Forgery:** This is seen as an important first step to reducing Internet vulnerabilities. To this end, it is important that the sender should not be able to fake the source of packets emanating from him. Cs3 is proposing an enhancement to the Internet Protocol (IP) called Path Enhanced IP (PEIP). With PEIP, a packet carries its own path information that is NOT controlled by the sender. More details about PEIP may be found in the Cs3 White Paper “*IP Changes to Eliminate Source Forgery”* [5].

- **Establishing Cooperative Neighborhoods:** Central to the idea of infrastructure reliability is the need for a group-level abstraction larger than a site, and, smaller than the entire Internet. A group of topologically adjacent routers that are similarly enabled (e.g., with PEIP and other useful capabilities) define a cooperative neighborhood. In Cs3's technologies, the cooperative neighborhood is used as the basis (much more effectively than a single site could possibly be) to provide enhanced collective security and reliability.

- **Fair Service Scheduling to Defend Against Distributed Denial of Service Attacks:** Cs3 has a patent-pending "fair-service" approach to defending against packet flooding and related DoS attacks that allows customers their fair, uninterrupted share of shared resources even in the face of attacks. More technical details maybe found in Cs3's White Paper “*A Fair Service Approach to Defending Against Packet Flooding Attacks on the Internet*” [6].

## 4. Analysis of Benefits and Costs

Using cooperative neighborhoods, one can accurately trace packet sources and even paths down to the LAN where they originate. Establishing large neighborhoods as described would have the following major benefits to all Internet users:

- **Defenses Against Packet Flooding Attacks:** Unlike the "smart filters" approach, Cs3's approach requires no updates to keep up with new modes of attack. This is a major advantage.

- **Forensics and Network Management:** Few tools exist to treat the Internet as a true global network utility where organizations can see where problems are originating, plan around apparent problems, etc. Large neighborhoods can form the foundation for such tools.

- **Mission Critical Utilities:** Neighborhoods that have eliminated source forgery enable a host of new services and products. Filtering based on accurate packet sources, smarter allocation schemes for resources, and other services are now possible.

The major issues raised by the Cs3 approach are as follows:

- **Size of Neighborhoods:** The larger the neighborhood, the more effective the elimination of source forgery and the more effective the DDoS defense. While some benefits accrue to individual sites with the Cs3 DDoS defense, it provides even better value when there are larger neighborhoods.

- **PEIP Technology Issues:** Issues of compatibility between IP and PEIP have been analyzed in detail [5], but these ideas could be refined further as users of Beta implementations and reviewers provide added feedback.

- **Costs of PEIP:** PEIP requires that packets carry path data. This raises issues of bandwidth and latency. Neither of these appears to present a real problem. See Cs3’s White Paper on Elimination of Source Forgery [5] for more detailed analysis.

Cs3's infrastructure technology does raise some practical adoption issues that are beyond the scope of this paper to discuss. The RFC process with the IETF will be used to facilitate wider adoption. The benefits of the Cs3 technology far outweigh the costs. An Internet which offers the above features *as a fundamental matter of protocol* will undoubtedly be more secure and robust for all its users.

## 5. Implementation Status

Cs3 is developing this technology using funding from Defense Advanced Research Projects Agency (DARPA) and the California Technology Investment Partnership (CALTIP). Implementations for IPv4 and IPv6 will be completed on different platforms. The major milestones of the project for the next few months are as follows:

- **Linux version released**: A Linux router and firewall that implement PEIP and fair service scheduling will be available for demonstrations and release later in Spring 2001.
- **Cs3 Internet Consortium formed**: A consortium of influential commercial companies, research laboratories, Department of Defense agencies, Universities, and Law Enforcement agencies will be evaluating and refining the Linux technology and will be early adopters of production versions. Specific announcements about consortium members will be made in Spring 2001.
- **RFC Before the IETF**: Cs3 aims to propose PEIP as a viable protocol to replace IP in Summer 2001. Comments are welcome from all readers as they review the documents cited herein.
- **Commercial versions in Fall 2001**: Versions of PEIP and fair service scheduling on commercial routers and firewalls are due for release in Fall 2001.

## 6. References

[1] CERT Advisories : http://www.cert.org/summaries/CS-2000-01.html

[2] WWW Security FAQ : http://www.w3.org/Security/Faq/wwwsf9.html

[3] CISCO Recommended Measures : http://packetstorm.securify.com/distributed/cisco-newsflash.htm

[4] Ingress Filtering : http://info.internet.isi.edu/in-notes/rfc/files/rfc2267.txt

[5] IP Changes to Eliminate Source Forgery : http://www.cs3-inc.com/sf.html

[6] A Fair Service Approach to Defending Against Packet Flooding Attacks on the Internet; http://www.cs3-inc.com/ddos.html