D. Project Description: CICI: RSARC: DDoS Defense In Depth for DNS

D.1 Introduction

Denial-of-Service (DoS) attacks and Distributed Denial-of-Service (DDoS) attacks are a continuing problem, with recent attacks exceeding 1 Tb/s [26]. Major attacks continue to cause extended outages to dozens of Internet services, and smaller attacks force universities, companies and organizations to cope with them weekly. Recent attacks have both misused DNS services for reflection, and have targeted and successfully brought down major DNS servers. DNS plays a major role in the Internet's critical infrastructure. Clients initiate nearly all service requests by first performing DNS look-ups and when DNS is unavailable most other reliant services experience a total outage.

This proposal, to the "Resilient Security Architecture for Research Cyberinfrastructure" program area of the "Cybersecurity Innovation for Cyberinfrastructure" solicitation, focuses on DDoS attacks that target both DNS root servers specifically, and DNS servers in general. While point-solutions exist for some attack variants, and the largest cloud providers can absorb some attacks by distributing large-scale resources around the globe, there are currently no effective solutions to defend important infrastructure from large-scale attacks at reasonable costs. We propose a *defense in depth* approach to Distributed Denial-of-Service attacks for DNS servers, called Deep Layers. Our defense integrates two existing research technologies with some DNS-specific filters to to *detect spoofed addresses* (§ D.3.2) and *prioritize traffic from known-good users* (§ D.3.4). These approaches filter out attack traffic, while protecting the majority of legitimate client requests. Deep Layers further includes a *scale-out to the cloud* (§ D.3.6) approach, which is triggered when filtering does not sufficiently reduce the load on the server. These steps address an array of increasingly sophisticated attacks, ranging from those we see today to those that would be possible in the future.

Deep Layers will be able to protect a range of DNS server configurations, including authoritative name servers, caching resolvers and root servers. We will deploy Deep Layers to *protect the B-root*, the DNS root server we operate here at USC. B-root is part of the Internet's critical DNS infrastructure, and is one of 13 root Domain Name Servers that ground the Internet's naming service (`.com`, `.edu`, etc.). We will further work with the tightly-knit community of DNS root server operators, to transition our technologies to other root servers. As a long-standing member of this small community we have unique access to other peers that may adopt our technologies once we have established success. We provide letters of collaboration from F-root and K-root in § J.4.

Our results will be published as open source, allowing anyone running DNS server software, including servers of any size, to benefit from the project's outcomes. The software will be released under the GPLv2 License to maximize re-usability of our and future results by the research community.

Our team consists of DNS and DDoS experts. Mirkovic has 15 years of experience in DDoS-defense [61, 57, 55, 58, 59, 66, 53]. Heidemann has studied DDoS detection [35], the effects of DDoS on B-root [64] and how to protect DNS servers against misuse [95]. Hardaker has years of experience in DNS service operation and DNS security and standardization [30, 31, 32, 22, 21, 28, 15, 16, 17, 29]. In addition, USC is committed to supporting evaluation and eventual deployment of this approach on the B-root service; both Hardaker and Heidemann are part of and manage the B-root operations team.