Georgia College & State University

Milledgeville, GA

Domain Name Service Procedures

Domain Name Service

Table of Contents

TABLE OF REVISIONS **3**

SECTION 1: INTRODUCTION **4**

1.1 Scope and Objective 4

1.2 Terms and Definitions 4

SECTION 2: DOMAIN NAME SERVER (DNS) SYSTEM SECURITY **5**

2.1 Internal DNS Security Standards & Procedures 5

2.2 External DNS Security Standards & Procedures 6

Table of Revisions

Original Date: May 6, 2013

Revision Number:	Description:	Date:	Revised By:

Section 1: Introduction

The Georgia College & State University's Division of Information Technology (DoIT) is the steward of the Georgia College domain. The domain is facilitated by Domain Name Servers (DNS) that translates Internet Protocol (IP) addresses into domain names. The servers are a critical part of the campus network infrastructure and Internet navigation. Because DNS data is meant to be public, preserving the confidentiality of DNS data pertaining to publicly accessible IT resources is not a concern. The primary security goals for DNS are data integrity and source authentication, which are needed to ensure the authenticity of domain name information and to maintain the integrity of domain name information in transit. Thus, the DoIT maintains DNS security procedures that regulates use and protects the DNS systems from associated threats.

1.1 Scope and Objective

The DNS security procedures provide guidance for maintaining data integrity and performing source authentication. The procedures optimize and standardize practices concerning both internal and external DNS systems at Georgia College. They also improve Georgia College's security posture by reducing threats posed by attackers who could attempt to gain information about the network and subsequently use that information to compromise other services. By anticipating threats and utilizing a split DNS system, DoIT circumvents attacks such as unauthorized zone transfers, denial-of-service, and domain spoofing.

1.2 Terms and Definitions

Domain- is most often used to refer to a domain zone, but it is also used to describe a zone or a domain name.

Domain Name System (DNS) - an internet technology used to convert domain names to corresponding IP addresses.

DNS Spoofing (cache poisoning) - occurs when an attacker sends a recursive query using a FALSE authoritative record to a 'victim' server for resolution. The 'victim' server caches the false or spoofed record. The victim's resolve continues to use the false record resulting in a potentially major security leak as information can be misdirected.

Split DNS: Internal hosts are directed to an internal domain name server for name resolution, while external hosts are directed to an external domain name server for name resolution.

DoIT (Division of Information Technology)

Section 2: Domain Name Server (DNS) System Security

2.1 Internal DNS Security Standards & Procedures

Pursuant to USG Internal DNS Standard	DoIT Procedure
5.9.1.4 (1)	DoIT maintains an internal DNS system.
5.9.1.4 (2)	DNS systems are physically secured, isolated from human traffic, and restricted to authorized personnel. • The system locations are monitored to detect smoke, moisture, and temperature. • Unauthorized users cannot gain access and there is no threat of casual interference. • Authorized users are always logged out and server log on restrictions only permit access to identifiable systems. To mitigate single node failures, DNS server clients are configured to utilize primary, secondary, and tertiary servers. DNS servers are single purposed and preparations have been made to replace servers in the event of failure.
5.9.1.4 (3)	The internal DNS consists of an internal host record. The addresses are monitored and defined by access control listing.
5.9.1.4 (4)	DoIT utilizes Microsoft Active Directory (AD) environments which employs dynamic DNS as an integral part of the system architecture. Domain controllers register their network service types in DNS so that other computers in the Domain can access them. Updates are manually conducted so that the AD servicers can write back information.
5.9.1.4 (5)	Microsoft products authenticate and authorize all users of Georgia College PCs and laptops. PCs and Laptops are not listed on the DNS automatically because they are on a Georgia College domain and must be listed by using Active Directory (AD).
5.9.1.4 (6)	All internal applications refer to the DNS server. This is in anticipation of IP address changes on the server side, so it will not need configuration modification on client side. The DNS system structure mitigates the risk of domain spoofing and cache poisonings.

Pursuant to USG Internal DNS Standard	**DoIT Procedure**
5.9.1.4 (7)	The internal DNS server is located on LAN segment that is different than users.
5.9.1.4 (8)	The internal DNS system does not access the Internet directly. The system does not query directly against root or external servers.
5.9.1.4 (9)	Queries to the Internet domain are forwarded to an external DNS.
5.9.1.4 (10)	The internal DNS cannot be accessed from an external DNS or the Internet.

Table 1: Georgia College's Internal DNS Procedures Pursuant to USG Requirement 5.9.1.4

2.2 External DNS Security Standards & Procedures

Pursuant to USG External DNS Standard	**DoIT Procedure**
5.9.1.4 (1)	DoIT maintains an external DNS located in a demilitarized zone (DMZ).
5.9.1.4 (2)	The external DNS system is protected by firewalls, TCP 53, and UDP 53.
5.9.1.4 (3)	The external DNS system does not contain any internal hosts. No exclusively internal name is listed in the external DNS.
5.9.1.4 (4)	The external DNS system only contains host records that can be accessed by the Internet, such as a web server, Internet application, mail server, etc.
5.9.1.4 (5)	Georgia College's DNS is able to access the Internet to perform a domain query. It has the capability to synchronize upon proper authorization.

Table 2: Georgia College's External DNS Procedures Pursuant to USG Requirement 5.9.1.4