

Exploring DNS Security

JAMES CAPUDER

Oberlin College

EREN GUENDEL

Oberlin College

JUANBI BERRETTA

Oberlin College

December 15, 2016

Abstract

The security of common internet protocols is an important issue when considering how to satisfy the requirements of security and privacy as technology becomes more integral to our daily lives. The components required to simulate a DNS lookup were implemented in Java. This simulation was used to attempt a common DNS cache poisoning attack, and explore methods for improving the security of DNS protocol.

I. INTRODUCTION

One of the most important requirements of any communication network, such as the internet or the United States Postal Service, is the ability to uniquely identify and locate participants of the network. This requirement is often met by assigning some form of address to participants: to determine the location to which an outgoing letter should be delivered, the sender must specify country of the recipient, what part of the country they live in, and finally the specific street/number combination at which the recipient resides. This system, however, was designed for human comprehension, and could be more concisely represented by numerical coordinates if readability was not an issue. A similar issue arises when considering the numerical Internet Protocol addresses (IP addresses) used to identify computers and resources connected to the internet: IP addresses are convenient for use in networking protocols, but are difficult for humans to memorize. The Domain Name System (DNS) is in place to allow individuals or companies to register readable domain names (www.google.com) that can be mapped to the IP addresses needed to locate certain computers on the network, and is fundamental to the functionality of the internet.

The specific DNS protocol we examine in this report is referred to as a client lookup, as

this protocol is vulnerable to an attack known as cache poisoning. A client lookup is initiated whenever an application on a client's computer sends a request that requires a domain name to be translated to an IP address. The application will first send a request to a domain name resolver, which will check its cache of recent lookups for a response to the request. If the cache contains an appropriate response, the resolver will return it to the sender of the request; if not, the resolver will send the request to the root name server. The root name server will check its cache, and either return a cached response, or tell the DNS resolver the location of the next name server it should query. This process is repeated until the resolver receives a final response, which it will cache and return to the client.

One might hope that such an important protocol adheres to the canonical computer security principles of C.I.A.¹. DNS lookups, however, do not

II. METHODS

Maecenas sed ultricies felis. Sed imperdiet dictum arcu a egestas.

- Donec dolor arcu, rutrum id molestie in,

¹**Confidentiality:** Only authorized parties should be able to view data; **Integrity:** Data should not be altered in any unauthorized fashion; **Availability:** Data should be available to and modifiable by authorized individuals.

Table 1: *Example table*

Name		
First name	Last Name	Grade
John	Doe	7.5
Richard	Miles	2

- viverra sed diam
- Curabitur feugiat
 - turpis sed auctor facilisis
 - arcu eros accumsan lorem, at posuere mi diam sit amet tortor
 - Fusce fermentum, mi sit amet euismod rutrum
 - sem lorem molestie diam, iaculis aliquet sapien tortor non nisi
 - Pellentesque bibendum pretium aliquet

Lorem ipsum dolor sit amet, consectetur adipiscing elit. Etiam lobortis facilisis sem. Nullam nec mi et neque pharetra sollicitudin. Praesent imperdiet mi nec ante. Donec ullamcorper, felis non sodales commodo, lectus velit ultrices augue, a dignissim nibh lectus placerat pede. Vivamus nunc nunc, molestie ut, ultricies vel, semper in, velit. Ut porttitor. Praesent in sapien. Lorem ipsum dolor sit amet, consectetur adipiscing elit. Duis fringilla tristique neque. Sed interdum libero ut metus. Pellentesque placerat. Nam rutrum augue a leo. Morbi sed elit sit amet ante lobortis sollicitudin. Praesent blandit blandit mauris. Praesent lectus tellus, aliquet aliquam, luctus a, egestas a, turpis. Mauris lacinia lorem sit amet ipsum. Nunc quis urna dictum turpis accumsan semper.

Text requiring further explanation².

III. RESULTS

Lorem ipsum dolor sit amet, consectetur adipiscing elit. Etiam lobortis facilisis sem. Nullam nec mi et neque pharetra sollicitudin. Praesent imperdiet mi nec ante. Donec ullamcorper, felis non sodales commodo, lectus velit

²Example footnote

ultrices augue, a dignissim nibh lectus placerat pede. Vivamus nunc nunc, molestie ut, ultricies vel, semper in, velit. Ut porttitor. Praesent in sapien. Lorem ipsum dolor sit amet, consectetur adipiscing elit. Duis fringilla tristique neque. Sed interdum libero ut metus. Pellentesque placerat. Nam rutrum augue a leo. Morbi sed elit sit amet ante lobortis sollicitudin. Praesent blandit blandit mauris. Praesent lectus tellus, aliquet aliquam, luctus a, egestas a, turpis. Mauris lacinia lorem sit amet ipsum. Nunc quis urna dictum turpis accumsan semper.

$$e = mc^2 \quad (1)$$

Lorem ipsum dolor sit amet, consectetur adipiscing elit. Etiam lobortis facilisis sem. Nullam nec mi et neque pharetra sollicitudin. Praesent imperdiet mi nec ante. Donec ullamcorper, felis non sodales commodo, lectus velit ultrices augue, a dignissim nibh lectus placerat pede. Vivamus nunc nunc, molestie ut, ultricies vel, semper in, velit. Ut porttitor. Praesent in sapien. Lorem ipsum dolor sit amet, consectetur adipiscing elit. Duis fringilla tristique neque. Sed interdum libero ut metus. Pellentesque placerat. Nam rutrum augue a leo. Morbi sed elit sit amet ante lobortis sollicitudin. Praesent blandit blandit mauris. Praesent lectus tellus, aliquet aliquam, luctus a, egestas a, turpis. Mauris lacinia lorem sit amet ipsum. Nunc quis urna dictum turpis accumsan semper.

IV. DISCUSSION

i. Subsection One

A statement requiring citation [Figueredo and Wolf, 2009]. Lorem ipsum dolor sit amet, consectetur adipiscing elit. Etiam lobortis facilisis sem. Nullam nec mi et neque pharetra sollicitudin. Praesent imperdiet mi nec ante. Donec ullamcorper, felis non sodales commodo, lectus velit ultrices augue, a dignissim nibh lectus placerat pede. Vivamus nunc nunc, molestie ut, ultricies vel, semper in, velit. Ut porttitor. Praesent

in sapien. Lorem ipsum dolor sit amet, consectetur adipiscing elit. Duis fringilla tristique neque. Sed interdum libero ut metus. Pellentesque placerat. Nam rutrum augue a leo. Morbi sed elit sit amet ante lobortis sollicitudin. Praesent blandit blandit mauris. Praesent lectus tellus, aliquet aliquam, luctus a, egestas a, turpis. Mauris lacinia lorem sit amet ipsum. Nunc quis urna dictum turpis accumsan semper.

ii. Subsection Two

Lorem ipsum dolor sit amet, consectetur adipiscing elit. Etiam lobortis facilisis sem. Nullam nec mi et neque pharetra sollicitudin. Praesent imperdiet mi nec ante. Donec ullamcorper, felis non sodales commodo, lectus velit ultrices augue, a dignissim nibh lectus placerat pede. Vivamus nunc nunc, molestie ut, ultricies vel, semper in, velit. Ut porttitor. Praesent in sapien. Lorem ipsum dolor sit amet, consectetur adipiscing elit. Duis fringilla tristique neque. Sed interdum libero ut metus. Pellentesque placerat. Nam rutrum augue a leo. Morbi sed elit sit amet ante lobortis sollicitudin. Praesent blandit blandit mauris. Praesent lectus tellus, aliquet aliquam, luctus a, egestas a, turpis. Mauris lacinia lorem sit amet ipsum. Nunc quis urna dictum turpis accumsan semper.

REFERENCES

- [Figueredo and Wolf, 2009] Figueredo, A. J. and Wolf, P. S. A. (2009). Assortative pairing and life history strategy - a cross-cultural study. *Human Nature*, 20:317–330.