Title: Towards secure name resolution on the Internet

Author: Christian Grothoff, Matthias Wachs, Monika Ermert, Jacob Appelbaum

PII: S0167-4048(18)30040-3
DOI: https://doi.org/10.1016/j.cose.2018.01.018
Reference: COSE 1280

To appear in: *Computers & Security*

Towards Secure Name Resolution on the Internet

Christian Grothoff, Ph.D.; Matthias Wachs, Ph.D.; Monika Ermert; Jacob Appelbaum

Highlights

• Introduction to name resolution on the Internet

• Analysis of privacy requirements for name resolution in light of contemporary attacks

• Characterization of a wide range of alternative name resolution protocols

Abstract

The Domain Name System (DNS) provides crucial name resolution functions for most Internet services. As a result, DNS traffic provides an important attack vector for mass surveillance, as demonstrated by the QUANTUMDNS and MORECOWBELL programs of the NSA. This article reviews how DNS works and describes security considerations for next generation name resolution systems. We then describe DNS variations and analyze their impact on security and privacy. We also consider Namecoin, the GNU Name System and RAINS, which are more radical re-designs of name systems in that they both radically change the wire protocol and also eliminate the existing global consensus on TLDs provided by ICANN. Finally, we assess how the different systems stack up with respect to the goal of improving security and privacy of name resolution for the future Internet.

Keywords: name resolution, privacy, future Internet, network architecture, technology and society

1. Introduction

On the net, close to everything starts with a request to the Domain Name System (DNS), a core Internet protocol to allow users to access Internet services by names, such as www.example.com, instead of using numeric IP addresses, like 192.0.2.137 or even worse 2001:DB8:4145::4242. Developed in the “Internet good old times” where privacy and security was not a concern, the contemporary DNS allows DNS operators to monitor user behavior and usage patterns, and exposes information about the existence and availability of most services on the Internet [1]. Consequently, it attracts all sorts of commercially-motivated surveillance and manipulation: For example, Google’s public DNS service permanently logs a dozen items about

Email addresses: christian.grothoff@bfh.ch (Christian Grothoff), wachs@net.in.tum.de (Matthias Wachs), ermert@ermert.info (Monika Ermert), j.appelbaum@tue.nl (Jacob Appelbaum)