An Opportunistic Encryption Extension for the DNS Protocol

Theogene Hakiza Bucuti
Department of Computer Science and Engineering
University of North Texas
Denton, TX, US

Ram Dantu
Department of Computer Science and Engineering
University of North Texas
Denton, TX, US

***Abstract*—Confidentiality for DNS transactions has been a low-priority concern in DNS security for a long time due to performance requirements for the functionality of DNS and the fact that data in the DNS is considered public. However, the information carried in DNS transactions, if collected and analyzed, can pose real threats to personal privacy. This makes DNS a good target for passive eavesdropping to collect data for many purposes some of which may be malicious. The protocol described in this document is intended to facilitate an opportunistic negotiation of encryption in the DNS to provide confidentiality for the last mile of DNS resolution. It defines procedures to discover encryption-aware servers and how to establish a relationship with them with minimum overhead.**

I. Introduction

The data in the Domain Name System (DNS) [1] is considered public and available for retrieval by anyone without restrictions [2]. However, the metadata in DNS transactions contains information that can put the end-user's privacy at risk [3]. In addition to the allegedly public nature of the retrieved data, another factor impeding early privacy initiatives is the highly-mediated structure of the DNS, which makes end-to-end encryption difficult. The protocol described here as well as the other proposals in the literature consider the hop-by-hop approach for encryption, with a minimum goal to protect at least the traffic between clients and their immediate resolvers.

II. Related work

A number of mechanisms have been proposed to counter passive eavesdropping of DNS traffic. "Confidential DNS" [4] proposes the use of a new resource record (ENCRYPT) for a server's public key that clients should fetch and use to encrypt either a shared secret or public key they use to encrypt a DNS query and for the server to use for the encryption of the DNS response. T-DNS [5] proposes using TLS to mitigate spoofing and denial-of-service attacks on DNS, in a similar way to STARTTLS in SMTP and IMAP for the use of an in-band negotiation to upgrade an existing TCP connection to TLS.

III. A proposed mechanism for opportunistic encryption of DNS messages

One of the ways in which the protocol proposed here differs from [4] is that the retrieval of the server's key passively happens as part of a normal DNS query in "d*iscovery mode*" to any server whose key is not yet known, so this way no message is wasted to fetch a key (that may not exist) and the client does not have to implement any retry-logic to discover encryption-aware servers.

In addition, the protocol supports an optional secret caching mechanism allowing a server to remember a recent client's key and thus allow re-using the client's secret key for encrypting subsequent requests instead of the server's public key. This relationship is established succeeding an exchange of a nonce word, and is valid for a limited amount of time.

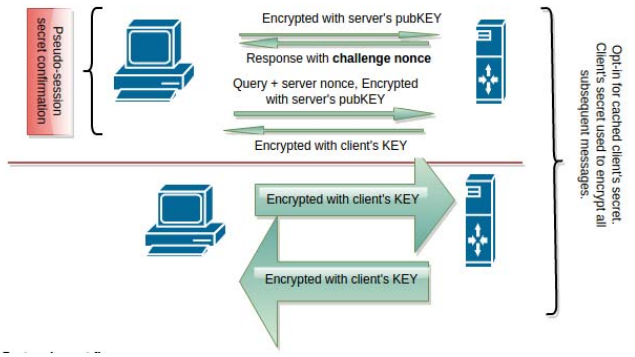

Fig. 1. Opting-in for a temporarily-shared secret key

IV. Conclusions and Additional Remarks

Compared to normal DNS, the proposed protocol will introduce a message size overhead due to the additional RRs, will require more computations for encryption/decryption, and force servers to keep more client states if client secrets are temporarily remembered. However, it is lighter than TLS-based approaches in that it maintains DNS's single-packet exchange nature and does not have the connection setup latency required by TCP and TLS. It is also important that the existing DNS security mechanisms be used to assure integrity and origin authentication for the server's public key retrievals.

References

[1] P. Mockapetris. "Domain names - concepts and facilities", RFC 1034, November 1987.

[2] R. Arends, R. Austein, M. Larson, D. Massey, and S. Rose. "DNS Security Introduction and Requirements", RFC 4033, March 2005.

[3] S. Bortzmeyer (April 2004). "DNS privacy considerations". IETF Draft.

[4] W. Wijngaards (September 2014). "Confidential DNS". IETF Draft.

[5] Z. Hu, L. Zhu, J. Heidemann, D. Wessels, A. Mankin, and N. Somaiya (August 2014). "T-DNS: Connection-Oriented DNS to improve Privacy and Security" ACM SIGCOMM, 2014, pp. 379-380.