Proposal: A Reproduction of "A Longitudinal End-to-End View of the DNSSEC Ecosystem"

Sean Decker
Stanford University
skdecker@stanford.edu

David Liedtka
Stanford University
dliedtka@stanford.edu

1 OVERVIEW

Our goal is to reproduce Chung et al.[2]. Chung et al. addresses the security problem of DNS cache poisoning, which is an exploitation that "poisons" DNS lookup servers to divert traffic away from legitimate servers to malicious ones[3]. DNSSEC was invented in the 2000s to address this problem, but Chung et al. shows that it had not been widely correctly implemented by 2017, leaving many DNS servers vulnerable.

Chung et al. examines issues related to DNSSEC from the server, domain-management side and from the client, resolver side. Chung et al. finds that 31% of domains that support DNSSEC fail to publish all relevant records required for validation and that 39% of the domains use insufficiently strong key-signing keys. Additionally, Chung et al. finds that although 82% of resolvers request DNSSEC records, only 12% of them actually attempt to validate them[2]. Like, Chung et al. we hope to examine DNSSEC from the server and client side.

We intend to reproduce Chung et al. as closely as possible, but our ability to collect measurements "longitudinally" (over time) is limited. Chung et al. collected measurements related to server-side DNSSEC deployment, many of which ran over a span of 21 months; clearly we are operating on a more condensed timeline. Thus, we will replicate Chung et al.'s experiments concerning client-side DNSSEC fully, but we will replicate abbreviated versions of measurements related to domain-side DNSSEC where necessary. We will fully reproduce Figures 2, 4, 10, and 12 and Tables 1, 2, 3, 4, 5, and 6, and we will reproduce abbreviated versions of Figures 3, 5, 6, 7, 8, 9, and 11.

In addition to being a good exercise for our own networking skill development, we believe that reproducing these results, which are now three years old, will provide valuable insight into whether usage and correct implementation of DNSSEC on the client and server side have increased since Chung et al.'s surprising findings were released.

2 TIMELINE

In order to successfully complete our project, we propose the following timeline.

By Friday, May 8, our goal is to have thoroughly read through and understood Chung et al. and to have gathered and understood other papers and resources that may have be helpful to us during our reproduction. We will also have looked through and understood Chung et al.'s publicly released data[1] and the tools we will need to reproduce the measurements and experiments.

By Friday, May 15, our goal is to have baseline reproduction code in place for server-side measurements. These are the measurements that Chung et al. collected over a 21 month span, so we would like to have them in place as early as possible to gather data for our abbreviated reproductions. Once we have a baseline in place, we will look to quickly expand to a full implementation of server-side measurement collection in order to begin collecting data.

By Friday, May 22, we will have submitted our intermediate project report, which we will have worked on during the preceding week by writing and writing code to reproduce the figures and tables concerning server-side measurement. Additional goals include beginning to collect data with our fully implemented server-side measurement collection, and starting to build baseline reproduction experiments for client-side DNSSEC. Additionally, we plan on reflecting on lessons learned to make any necessary modifications to our plan for the rest of the project.

By Friday, May 29, our goal is to have fully implemented our client-side DNSSEC experiments. We will run our client-side experiments and write code to reproduce the tables associated with the experiments.

By Friday, June 5, our goal is to have finished collecting our server-side measurements and begun work on our final report and presentation. We will use the rest of the time before the respective due dates to finish our presentation before June 9 or June 10 and to finish our final report by June 11. We will also use this remaining time to resolve any unanticipated issues to our progress that we should encounter.

REFERENCES

[1] Taejoong Chung, Roland van Rijswijk-Deij, Balakrishnan Chandrasekaran, David Choffnes, Dave Levin, Bruce M Maggs, Alan Mislove, and Christo Wilson. [n.d.]. A Longitudinal, End-to-End View of the DNSSEC Ecosystem. https://securepki.org/sec17.html. Accessed: 2020-05-03.

[2] Taejoong Chung, Roland van Rijswijk-Deij, Balakrishnan Chandrasekaran, David Choffnes, Dave Levin, Bruce M Maggs, Alan Mislove, and Christo Wilson. 2017. A Longitudinal, End-to-End View of the {DNSSEC} Ecosystem. In *26th {USENIX} Security Symposium ({USENIX} Security 17)*. 1307–1322.

[3] Steve Friedl. 2008. An illustrated guide to the kaminsky dns vulnerability. *Unixwiz. net Tech Tips, August* (2008).