ComEX

IEICE Communications Express, Vol.3, No.10, 305–310

DNSSEC simulator for realistic estimation of deployment impacts

Yuji Sekiya[1a)], **Tomohiro Ishihara**[2], **and Hajime Tazaki**[1]

[1] *Information Technology Center, The University of Tokyo, 2–11–16 Yayoi, Bunkyo-ku, Tokyo 113–8658, Japan*

[2] *Graduate School of Arts and Sciences, The University of Tokyo, 3–8–1 Komaba, Meguro-ku, Tokyo 153–8902, Japan*

a) *sekiya@nc.u-tokyo.ac.jp*

Abstract: DNS is one of important infrastructures on the Internet. If widely-known domain names are forged by DNS spoofing, a number of users have the potential to be forged and lead to phishing sites. In order to protect users, DNSSEC is an important technology. However, DNSSEC is not widely deployed now because the deployment has side effects in operator's point of view. It is anxious for DNS operators to enable DNSSEC without creditable estimations of its impacts. In this paper, we propose DNSSEC simulator which can estimate the impacts. Our DNSSEC simulator can estimate and simulate the impacts using actual DNS queries, DNS topology, and actual DNS implementations. Moreover, there is no need of knowledge of DNS simulation. The simulator estimates the impacts easily by just providing DNS query log. The software can contribute the deployment of DNSSEC and achieving safe DNS world.

Keywords: DNSSEC, DNS, simulator, ns-3

Classification: Internet

References

[1] G. Husuton, "Measuring DNSSEC use," RIPE67, https://ripe67.ripe.net/presentations/presentation-archive/, Athens, Greece, Oct. 2013.

[2] E. Osterweil, D. Massey, and L. Zhang, "Deploying and monitoring DNS security (DNSSEC)," Proc. of Computer Security Applications Conference 2009, pp. 429–438, Honolulu, U.S.A., Dec. 2009.

[3] A. Guillard, "DNSSEC operational impact and performance," Proc. of the International Multi-Conference on Computing in the Global Information Technology 2006, pp. 63–70, Bucharest, Romania, Aug. 2006. DOI:10.1109/ICCGI.2006.27

[4] K. Rikitake, H. Nogawa, T. Tanaka, K. Nakao, and S. Shimojo, "An analysis of DNSSEC transport overhead increase," IPSJ SIG Tech. Reports 2005-CSEC-28, vol. 33, pp. 345–350, 2005.

[5] H. Tazaki, F. Uarbani, E. Mancini, M. Lacage, D. Camara, T. Turletti, and W. Dabbous, "Direct code execution: revisiting library OS architecture for reproducible network experiments," ACM CoNEXT 2013, pp. 217–228, December 2013. DOI:10.1145/2535372.2535374

[6] T. Ishihara, H. Tazaki, and Y. Sekiya, "Design and implementation of DNSSEC

DOI: 10.1587/comex.3.305
Received September 8, 2014
Accepted September 18, 2014
Published October 16, 2014

simulator using unmodified real implementations," IEICE Tech. Report, vol. 113, no. 240, IA2013-27, pp. 7–12, 2013.

1 Introduction

DNS Security Extensions (DNSSEC) is a security enhancement of Domain Name System (DNS). It is designed to guarantee the origin of DNS answers. If DNSSEC is deployed widely, users and applications are protected from the forged attacks, so there are advantages for both users and applications. However, DNSSEC is not deployed widely [1, 2], especially in DNS resolver because there are two big barriers of DNSSEC deployment. In order to achieve the secure DNS world, the barriers should be removed and the research can help to remove the barriers.

1.1 DNSSEC deployment

DNSSEC has some potential barriers regarding its deployment. The first point is that DNSSEC requires more exchanging messages between DNS servers than non-DNSSEC one. It means that a DNSSEC capable DNS server consumes more bandwidth than a non-DNSSEC capable DNS server. The second point is that a DNSSEC capable DNS server requires more computing resources than a non-DNSSEC one because DNSSEC requires to calculate digital signatures to validate DNS data. A DNS resolver has to validate each Resource Record (RR), and an authoritative DNS server has to prove the existence or non-existence of each RR.

The two points may make major impacts on performance of DNS servers and network bandwidths when the DNS operators enables DNSSEC on their environments. It is anxious for DNS operators to make such changes in the existing environments without evaluation and estimation of its impacts. In order to figure out the impacts of enabling DNSSEC for DNS operators, it is mandatory and useful to evaluate the impacts on their actual DNS environments, or appropriately-approximated DNS environments to theirs. There are a few existing research [3, 4] for estimating the impacts of enabling DNSSEC, however, there is neither productive method nor good tool for estimation and evaluation of DNSSEC.

1.2 Approaches to the problems

When DNSSEC is introduced and deployed in the existing DNS environments, the amount of DNS traffic is increased and the CPU loads of DNS server is exhausted. It is not so difficult for DNS operators to try to build a test environment of DNSSEC. Maybe the test environment has a closed network, a DNS server or a few DNS servers. They can easily make measurements of impacts on their test environments; the CPU utilization and network bandwidth of DNSSEC messages by some test tools such as "queryperf" by ISC and "dnsperf" by Nominum. However, it is little use for DNS operators to estimate such the impacts on test environment. Because DNS database has a tree structure and DNS servers are linked by zone delegations from an upper zone to lower zones (where a zone consists of a name space managed by a DNS server), so the impacts will be affected and changed by (1) exchanging messages by the queries from clients and (2) the implementation of

DOI: 10.1587/comex.3.305
Received September 8, 2014
Accepted September 18, 2014
Published October 16, 2014

DNS servers which have RR queried, and (3) network situation between DNS servers.

There are a few network simulators such as ns-2, ns-3, OPNET, GNS3, and NetSim. Also there are some server simulators such as Paessler and SimLab. Using the simulators DNS operators can estimate and simulate the impacts to a relatively limited extent. Even if only one client queries a name, several DNS servers will have to exchange messages and return an answer to a client. If a number of clients query many kinds of name, a lot of DNS servers may have to exchange messages, so the test environment or simulation environment should include a lot of DNS servers for a realistic estimation.

As our preliminary survey, we monitored the DNS packets on a DNS resolver located in an university. There are about 20,000 unique names, about 12,000 zones, and 788 unique clients are observed in only 6 minutes. The total number of queries from clients are about 90,000. Over thousands of DNS servers may be involved in the captured situation. It is not easy to build such the environment for testing and using actual queries for estimation.

In order to solve the above difficulties, we design our simulator to fulfill the conditions below.

- Actual DNS queries are applicable for the simulation,
- actual DNS implementations can be executed the simulator, and
- any DNS operator can run and estimate the impacts easily.

2 Design and implementation of the DNSSEC simulator

According to our goals described before, we designed and implemented our simulator. As shown in Fig. 1, the simulator is composed of two modules, one is Direct Code Execution (DCE) [5] extension of ns-3 network simulator, and the other is the makeup tool which can make zones, DNS servers, and simulation scenarios, called "CreateZones" [1].

As we described in our previous paper [6], we adapted ns-3 and DCE for the base framework of our simulator. The DCE helps us to simulate with actual DNS implementations such as `bind9` and `unbound` on ns-3 without any modification. The CreateZones tool generates zone definition files, DNS configuration files for DNS servers, and DNS query scenarios sent by clients. The files are generated by providing a few simulation parameters or generated automatically from query log files of bind9 and/or pcap files from tcpdump.

When DNS operators try to start the estimation of DNSSEC impacts, the first step of the simulation is creating zone files, DNS configuration files, and query scenarios from query log or pcap files. The CreateZones tool generates the files following the procedure as shown in Fig. 2.

The second step is loading the files generated by CreateZones into the ns-3 DCE simulator, then run the scenarios. As a result, the simulator outputs pcap files of exchanging DNSSEC packets following the scenarios. Using the output pcap and trace files, DNS operators can find the growth of network bandwidths and the delay of DNS responses.

[1] https://github.com/shored/createzones/

DOI: 10.1587/comex.3.305
Received September 8, 2014
Accepted September 18, 2014
Published October 16, 2014

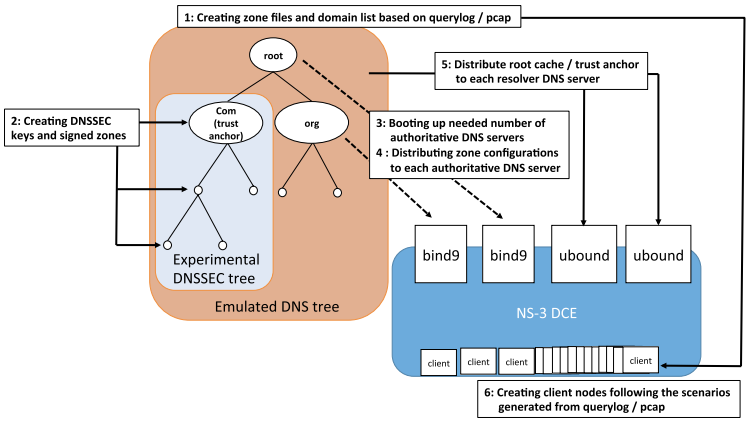


Fig. 1. The design overview of the DNSSEC simulator.

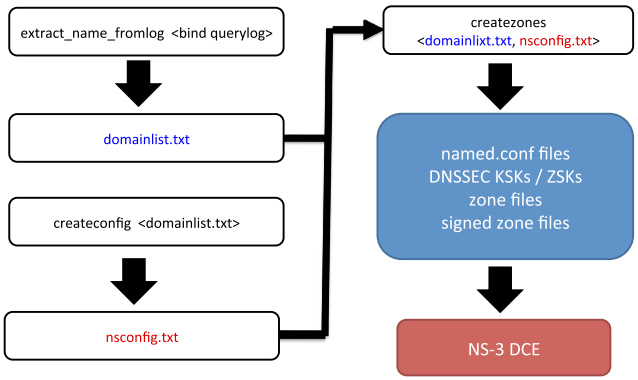


Fig. 2. The procedure of CreateZones.

3 Evaluation of the DNSSEC simulator

In order to evaluate the validity of our DNSSEC simulator, we performed a simulation using the simulator and show the potential benefit to understand the impact on DNSSEC deployment.

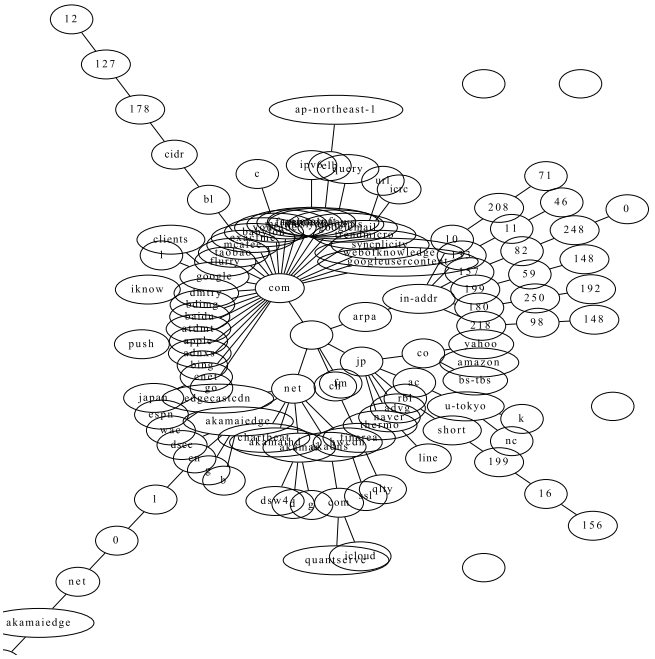
Response time impact on enabling DNSSEC validation

The objective of this experiment is to understand the impact of DNSSEC deployment by measuring the delay of name resolution with and without DNSSEC.

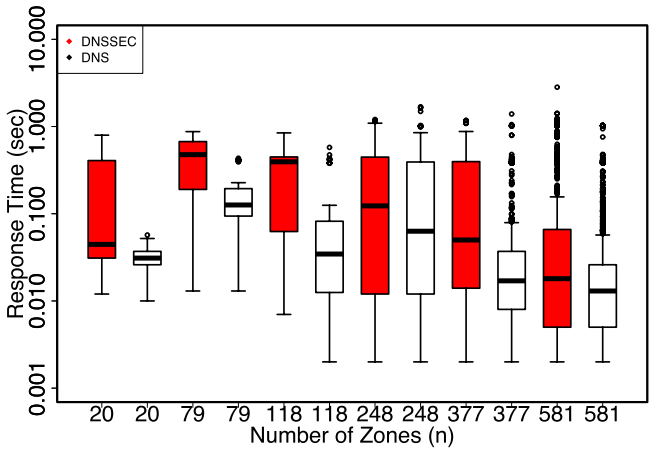
Our experimental setup is trying to follow an *actual* environment as much as possible. For the traffic of DNS queries, we used `dig` command to generate bunch of DNS queries, for the cache and authoritative DNS servers, we used `bind9` and `unbound`, which are defacto DNS implementations. For the network topology, we reproduced a DNS topology which is included in recorded queries (i.e., query log) observed at a cache server. We measured the response time of each DNS query with 1) different number of zones (from 20 to 581) included in query log and 2) enabling and disabling DNSSEC validation.

Fig. 3(b) represents the response time of each DNS query in function of the number of name zones in the DNS topology as shown in Fig. 3(a). With each number of zones, we injected DNS queries by `dig` command with the timing of recorded querylog. With this simulation, we extended the clock of simulation engine (in ns-3) in order to reflect the processing time of each application code: in

DOI: 10.1587/comex.3.305
Received September 8, 2014
Accepted September 18, 2014
Published October 16, 2014



(a) Simulated DNS topology based on recorded DNS query (the number of zones is 118).



(b) Response time in function of the number of name zones.

Fig. 3. Topology and the result of simulated DNS experiment.

our case, the duration of DNSSEC validation process is included in the result of response time. Thus, the result of response time of DNSSEC query is meaningfully longer than the one of DNS: in case of the number of zones is 581, the mean and maximum response times of DNSSEC query are 0.13 and 2.83 seconds while the one of DNS query are 0.05 and 1.03 seconds, respectively. The maximum response time of a query with 581 zones is due to the current implementation of CreateZones which simply splits labels of domain names by period and does not consider the actual zone definition, resulting long depth of DNS tree as presented in Fig. 3(a). In order to precisely reproduce the zone definition, we need to ask the operated DNS server for the particular record but this will be a future work of this paper.

Note that as the number of zones and transmitted queries are increased, the mean response time becomes shorter than the one of small number of zones. This is

DOI: 10.1587/comex.3.305
Received September 8, 2014
Accepted September 18, 2014
Published October 16, 2014

due to the cache effect of DNS servers since more queried domain name increases, more queries share the same domain name, resulting fewer message exchanges among DNS servers.

Our simulator successfully replayed a DNSSEC scenario based on the measured DNS traffic and observed a possible overhead when we are using DNSSEC validation.

4 Conclusion

DNSSEC is an important technology to achieve safe DNS world. However, it is anxious for DNS operators to enable DNSSEC on their DNS servers without creditable estimations because enabling DNSSEC has a few drawbacks from an operator's point of view.

We have designed and implemented the simulator so that DNS operators can perform simulations and get the results without any difficulties. Also the simulator has flexibility of the scenarios. Even if DNS operators do not know about the ns-3 simulator itself, they can run simulation only by providing DNS query log files from their DNS servers. If a user knows about ns-3 simulator, he can simulate any situations of DNS servers on the simulator.

We released the software as an open-source software[2]. Using the software, anyone may be able to estimate DNSSEC impacts on their emulated DNS environments. It is very helpful for DNSSEC deployment, so we conclude that we contribute a progress of safe DNS world with DNSSEC.

Acknowledgments

This research is supported by JSPS KAKENHI Grant-in-Aid for Scientific Research (C). The Grant Numbers are 23500080 and 26330101. Also this research is a part of NECOMA Project[3] and has been supported by the Strategic International Collaborative R&D Promotion Program of the Ministry of Internal Affairs and Communication, Japan, and by the European Union Seventh Framework Programme (FP7/2007-2013) under grant agreement No. 608533 (NECOMA).

[2]http://dnssec.sekiya-lab.info/
[3]http://www.necoma-project.jp/

DOI: 10.1587/comex.3.305
Received September 8, 2014
Accepted September 18, 2014
Published October 16, 2014