Health Evaluation of a Domain Name System Based on the Analytic Hierarchy Process

Jian Jin[1,2,3], Zhiwei Yan[1], Jong-Hyouk Lee[4], Guanggang Geng[1]

[1] China Internet Network Information Center,
[2] University of Chinese Academy of Sciences,
[3] Computer Network Information Center, Chinese Academy of Sciences, China
[4] Department of Software, Sangmyung University, Korea
{jinjian, yanzhiwei}@cnnic.cn, jonghyouk@smu.ac.kr, gengguanggang@cnnic.cn

Abstract

As the vital infrastructure of the Internet, the Domain Name System (DNS) is important from any aspect of Internet actors with the explosive increases of connected things and deployed applications. However, how to monitor and evaluate the healthy state of the DNS is an emergent and difficult issue. In this paper, we propose an Analytic Hierarchy Process (AHP) based DNS evaluation method. We adopt the Point of View (PoV) idea proposed by Global Cyber Security Center (GCSEC) and extend their metric sets for more comprehensive understanding of the DNS health. The AHP is introduced to set the weights for different metrics based on the threat scenario or special PoV. We introduce a monitoring platform with two examples of the actual procedure. The results show that we can adopt this method in any use case for the DNS health evaluation and improvement.

Keywords: DNS, Health evaluation, AHP, Security

1 Introduction

The global Domain Name System (DNS) [1] is a fundamental and even more, an essential building block of the traditional Internet and the future Internet of Things (IoT). In the current Internet, DNS provides mappings between domain names used by people and the corresponding IP addresses required by network protocols. The data for this mapping is stored in a tree-structured distributed database where each name server is authoritative for a part of the naming tree.

In addition, as we move forward towards ambient intelligence environments where most devices are connected to seamless and ubiquitous networks, inter-enterprise interoperability becomes an essential prerequisite. Integrated complex networks, composed of a huge amount of different types of objects, form the so-called IoT [2]. In order to identify each object in the IoT, the object naming scheme is used to uniquely identify the object. And the IoT name resolution service aims to resolve the given object identifications for end users or software agents to derive the information resource related to the given identifications respecting their access rights.

However, due to the historical and actual reasons, many different object naming and resolution standards are proposed, such as the Electronic Product Code (EPC) [3] and ubiquitous Code (uCode) [4]. They use different coding rules to identify the object and adopt the different resolution schemes, accordingly. However, because DNS is the most mature and widespread infrastructure in the current Internet for the name resolution (e.g., until September 2015, the total number of second level domain names is about 150,000,000 [5]), it is the first choice for the IoT name resolution architecture. For example, the EPCglobal, which is the most successful IoT standardization organization, makes use of DNS to support the EPC resolution. Technically, its Object Naming Service (ONS) [6] is a subset of the DNS. The idea is to first encode the EPC into a domain name while preserving its structure and field values, then to use the existing DNS protocol and delegation procedures.

In a word, no matter in the traditional Internet or in the future ubiquitous IoT environment, DNS was and will still be a critical information infrastructure, resolving billions of queries per day as a hierarchical information system [7-8]. DNS is the core for the normal and correct operation of most of Internet services and then the problem of the DNS health and its impact on the different roles in the Internet was discussed largely by the community as a hot and important topic.

In about 2010, The Internet Corporation for Assigned Names and Numbers (ICANN) proposed the concept of DNS health, in order to define whether the DNS system is healthy or not, adopting the concept of human health [9]. But it is just an abstract-level concept, without any suggestion about how to evaluate

*Corresponding Author: Jong-Hyouk Lee; E-mail: jonghyouk@smu.ac.kr
DOI: 10.3966/160792642018011901003

it in reality. In particular, as DNS system is consisted with multiple levels from the root to the top, second and lower levels, besides, different operators and users have different views on the DNS system (no matter it is a whole view or part view), it is very difficult to consider what metrics should be considered to evaluate the health of DNS system and it is more difficult to integrate different metrics together to quantify the health status of the DNS system.

Under this light, the first workshop on DNS health and security (DNS EASY-2011) [10] was organized by the Global Cyber Security Center (GCSEC) [11], in cooperation with the ICANN and the DNS Operation Analysis and Research Center (DNS-OARC). This workshop aims to bring together researchers and professionals from academia, industry and governmental agencies, and representatives from different DNS stakeholders to discuss all different aspects of the DNS Health and Security (HEALTH) and its impact on the whole Internet[1]. Besides, GCSEC proposed several documents in order to present how to evaluate the health and security states of the DNS system. In 2012 [12], some researchers from GCSEC also proposed two methods to aggregate the DNS HEALTH related metrics and in one more step to verify the health level of DNS service. However, how to set the weights for the multiple considered metrics is still blank in this area and what is just our main contribution in this paper. We here aim to introduce the new evaluation metrics and method for the DNS health. But we mainly describe the idea with the security performance for clarity and specificity because health is a broader concept, which includes the security as just one aspect.

The rest of this paper is organized as follows. Section 2 describes the related work. Section 3 explains our proposed scheme in detail and Section 4 presents two examples of our proposed scheme. Finally, Section 5 concludes.

2 Related work

The DNS is a distributed information service accessed by billions of Internet users and more and more things. Then, the Security, Stability and Resilience (SSR) of DNS system are very important for the correct operation of most of the services and applications in the current and future Internet. DNS system firstly served as a tree-structured system without any protection on the exchanged information. With the growth of Internet, the DNS system is more and more important because more and more information is stored in this tree. Then the community proposed the Domain Name System Security Extensions (DNSSEC) [13-15] to guarantee that the DNS information was generated from the authenticated source and not modified during transmission. Based on DNSSEC, many new functions were developed on DNS to provide SSR protections (e.g., privacy, anti-DDoS attack). But the problem of how to evaluate the DNS health is still unsolved and more complex with these new features.

Although there are many studies about the DNS measurements and performance evaluation [16-18], only few exist regarding the DNS SSR analysis. In the second Symposium on DNS SSR [6], a report was released which was about the DNS SSR measurement. In this report, the DNS health is affected by two aspects: performance and resiliency. Additionally, the DNS health proposed in this report should be evaluated from six key indexes: availability, coherency, integrity, resiliency and speed. Of course, Stability is very important to check whether the DNS system works normally [19]. But as security has become an essential element of DNS functions, whether the DNS system is able to cope with different malicious activities must be considered to comprehensively evaluate the health status of DNS system.

Based on these important studies, GCSEC launched the Measuring Naming System (MENSA) project, which aims at defining a set of metrics and a related algorithm to quantify the DNS health level of different functions and from different views. Based on the results of this project, it is recognized that the difficulty about DNS health evaluation is the unbalance between the DNS usage and DNS measurement: every users involved in the DNS has to use every part of the DNS system in order to retrieve the necessary information, however, the global DNS system is operated and managed by different stakeholders and they just locally measure and evaluate the DNS function. Then it is difficult to specify the metrics and procedures to evaluate the health of global DNS system.

In order to define the boundaries, five Points of View (PoVs) to evaluate the DNS health have been defined by the GCSEC [20]. In addition, some metrics are defined in order to quantify the health level of the DNS system [21]. The metrics they proposed are intended to evaluate the DNS health by measuring the DNS from three dimensions: Vulnerabilities, Security, and Resiliency. A set of measurement techniques and tools are used to gather information needed to compute these metrics. How to implement the measurement depends on two factors: (a) what can be measured from which point; and (b) the time horizon of data collection (e.g., seconds, hours, days or months). These problems are described in [22]. In SATIN 2012, GCSEC additionally proposes two methods for the metric aggregation: the session-based scheme and the metric-based scheme [23]. The session-based scheme is simple and provides a simple way to cope with the error of measurement. But it is not tolerant of any data

[1] Although the focus of this paper is the same as DNS-EASY workshop, we herein denoted the concept of DNS Health and Security (HEALTH) as DNS Health for short.

missing; otherwise the computation is not possible without losing accuracy. In addition, the metric-based scheme is more complex than the session-based method. Moreover, the final error will be aggregated, by the measurement error of each metric. With the explosive increase of the new generic Top-Level Domain (gTLD), ICANN recently seeks community input to facilitate the creation of a gTLD Marketplace Health Index. This Index will analyze the overall health and diversity of the global gTLD marketplace [24]. Although there are some basic studies on the DNS health evaluation, how to set the weights for the considered metrics is a problem still up in the air.

3 DNS Health Evaluation

In this section, we present our DNS health evaluation method in detail.

3.1 Points of View

As GCSEC analyzed, the evaluation of DNS health should be executed from different PoV according to the special actions and focuses of different DNS actors. Specially speaking, a PoV is intended as the perspective of a DNS actor/component in observing, using, operating and influencing the DNS [23]. Each PoV has a different perception of DNS health. The PoV has influence on the system model used to evaluate DNS health, on the metrics used to quantify DNS health and on how those metrics should be measured. The possible PoV they proposed are list in Table 1.

Table 1. PoVs of the DNS security evaluation

PoV type	Related elements	Operations
End-user	Application, Stub resolver and Network	DNS lookup process
Application Service Provider	ASP, Stub Resolver and Network DNS Sub-System and the Intranet	DNS lookup process DNS sub-system management
Resolver	Forwarder and Network Full resolver and Network	Indexes of external resolvers Indexes of network and name servers
Name Server	Master	DNS lookup process and the zone management process
	Slave	DNS lookup process and the zone transfer process
Zone	Name servers, Databases and Registrant	DNS lookup, the Zone transfer and the database update and management routines
Global	All elements above	All processes above

The six points of view we adopt are: End-User PoV, Application Service Provider (ASP) PoV, Resolver PoV, Name Server PoV (including the Master server and Slave server), Zone PoV and Global PoV. From each of the above PoVs, it is possible to directly observe and measure the behavior of some DNS components while it is not directly feasible to measure other not accessible components.

3.2 Metrics

GCSEC also proposed some metrics to be used to evaluate the health of the DNS from three dimensions: Vulnerabilities, Security, and Resiliency.

(1) The most common DNS vulnerabilities, present in many threats scenarios such as those discussed in [25] are: Cache Poisoning, Distributed Denial of Service (DDoS), Response Modification, Route Injection, and Origination Modification. Such hazards, and many more, can be classified into three main threats categories as reported in [26]: Data corruption, DoS and Privacy Violation. In this document, vulnerability metrics are organized as five categories which are corresponding to the DNS vulnerabilities mentioned above.

(2) Metrics about security aspect are defined as the ability of the DNS system to limit or protect itself from malicious activity has not yet to be defined. But with the growing deployment of DNSSEC, the most serious security issues in DNS (e.g., cache-poisoning, DNS hijacking) can be solved.

(3) DNS Resiliency is the ability of the DNS system to effectively respond and recover to the safe status when disruption happens (e.g., response and recovery after a distributed denial of service attack). DNS Resiliency can also be described as the ability of the DNS to provide and maintain an acceptable level of service in face of faults and challenges to normal operations.

Based on the metrics defined by GCSEC, we propose a set of metrics in Table 2 that, taken together, can contribute to the evaluation of DNS health readiness with respect to a possible set of scenarios from different PoVs[2]. For example, as the most typical protocol vulnerability, cache poisoning may happen on resolver, the name server should not open the recursive service and zone file transfer may fail from the perspective of zone manager. In order to evaluate the DoS attack, many metrics should be considered, such as the number of queries per second, incoming bandwidth consumption, rate of repeated queries and

[2] The details of the metrics proposed by GCSEC can be found in [12].

so on. The reason we only select the Resolver PoV, Name server PoV and Zone PoV here is that these three aspects cover the main functions of DNS (e.g., recursive service and authoritative service) but not involve in any other functions only having relationship with DNS (e.g., upper layer application, user API with DNS and network).

Among the metrics list in Table 2, we add several new metrics except the metrics defined by GCSEC as shown in Table 3. They are Open recursion, Service independency, Time synchronicity, Port randomness, Server redundancy and Querying latency. These six new metrics are mainly from our daily operation experience and security experiments of DNS service.

Table 2. Metrics of the DNS health evaluation

	Resolver	Name Server	Zone
Repository Corruption		Data staleness Zone drift/Zone thrash Data staleness duration Parent/Child data coher. Glue inconsistencies	Data staleness Zone drift/Zone thrash Data staleness duration Parent/Child data coher. Glue inconsistencies Zone inconsistencies
Protocol issues	Cache poisoning Port randomness	Open recursion Zone transfer failure Zone transfer protection Service independency	Zone transfer failure Zone transfer protection Service independency Time synchronicity
DoS	Var. of req. per sec. Var. of query type distr. Incoming band. cons. Rate of repeated queries Traffic tolerance Data pollution Incoming traff. var. Querying latency	Var. of req. per sec. Var. of query type distr. Incoming band. cons. Rate of repeated queries Traffic tolerance Data pollution Incoming traff. var. Geographical DoS effect. Server redundancy Querying latency	
Information Exposure		Zone walkability RR type info. leakage	Zone walkability RR type info. leakage
DNSSEC	Data availability DNSSEC supporting	DNSSEC supporting	Keyset availability Verifiability
Resiliency	Mean time to incident dis. Ope. time between failures Operational availability Operational reliability Average recovery speed	Mean time to incident dis. Ope. time between failures Operational availability Operational reliability Average recovery speed	

Table 3. Newly defined metrics

	Description	Meaning
Open recursion	To test whether the authoritative server opens the recursive function	If so, the authoritative serer can be easily attacked by the DoS traffic
Service independency	To test whether the authoritative server also opens other ports for the applications except DNS	More ports opened, the service of DNS is less stable due to the effects of other applications
Time synchronicity	To test whether the time is synchronized between multiple authoritative servers in a same zone	If not, some operations, such as TSIG, may not be successfully executed
Port randomness	To test whether and to what extent the recursive server randomizes the port of recursive request message	If the port randomness is bad, the poisoning attack to the recursive server has high possibility
Server redundancy	To test how many servers exist in a zone	More authoritative server means the service stability and performance of the related zone is better
Querying latency	To measure the latency of the DNS service	If the latency is too long, the server may be DoS attacked

3.3 AHP Based Evaluation

Since a number of metrics must be considered in order to calculate the health level of DNS service from different PoV, the AHP [27] method is employed. The AHP method is chosen because of its ability to vary its weighting between each metric, which fits well with our framework that requires the decision making process to be different for every individual PoV and scenario. It can be well used to calculate the qualitative DNS health and the similar issues [28-29] and was originally proposed by Saaty in [30] to support decision making in management science. The AHP method includes three major steps. Step 1: Create the input values by pair-wise comparisons of decision elements. Step 2: Estimate the relative weights of the decision elements. Step 3: Combine the relative weights to determine the ranking of the different decision alternatives[3].

Step 1. In our use case, q represents the security quality ranking of the DNS service from a special PoV with regard to a special threat scenario. $A(i \times j)$ matrix, denoted as A, is created using the comparisons with elements $a_{ij} > 0$, indicating the importance of metric i relative to metric j as shown in equation 1.

$$A = \begin{pmatrix} a_{11}\ a_{12}\ a_{13}\ \ldots\ a_{1j} \\ a_{21}\ a_{22}\ a_{23}\ \ldots\ a_{2j} \\ \vdots \\ a_{i1}\ \ a_{i1}\ a_{i1}\ \ldots\ a_{ij} \end{pmatrix} \quad \textbf{(1)}$$

Obviously, $a_{ij} = 1$ when $i = j$, while $a_{ij} = 1/a_{ji}$, which reflects the reciprocal importance of metric j relative to metric i. In our use case, the metric has two-fold meanings related to DNS health (for example about security): the first aspect is that we should evaluate the seriousness of the metric related threat and the second aspect is that we should evaluate the difficulty of the successful attack using this metric shortcoming. That means the comparison matrix should be constructed with the above two aspects in consideration.

Step 2. After constructing the matrix of comparison, the next step is to determine the weights of the metric, in which, w_i is the weight of metric i in the weight vector $w = [w_1, w_2, w_3, \ldots w_n]$ for n metrics. The objective is to recover vector w from matrix A by finding the solution for some value u showed in equation 2.

$$A \cdot w^T = u \cdot w^T \quad \textbf{(2)}$$

In order to determine w_i, a numerical solution is used which starts with normalizing each column j in A such that

$$a_{ij}' = \frac{a_{ij}}{\sum_{i=1}^{n} a_{ij}} \quad \textbf{(3)}$$

Next, each row i in a' is summarized into a vector with elements

$$a_i'' = \sum_{j=1}^{n} a_{ij}' \quad \textbf{(4)}$$

Finally, the vector w is obtained as

$$w_i = \frac{a_i''}{\sum_{j=1}^{n} a_j''} \quad \textbf{(5)}$$

Step 3. The last step is to calculate the security value of the DNS service and which can be written as

$$q = \{N_1(M_1), N_2(M_2) \ldots N_{n-1}(M_{n-1}), N_n(M_n)\} \cdot w^T \quad \textbf{(6)}$$

where $N_i(M_i)$ is the normalization function of parameter M_i. Normalization is needed to ensure that the sum of the values in different units is meaningful. Because different metrics have different value space and security meanings, their normalization functions are different. q is always larger than 1 and the higher the value of q means that the security performance of the DNS service is better.

• Based on the above algorithm, two kinds of evaluation can be made with different granularities:

• Based on the DNS threat scenario

In this case, we should select the metrics having relationship with that kind of DNS threat. The procedure is illustrated above.

Based on the PoV. In this case, the security values corresponding to the threat scenarios from a special PoV is used as the input of the comparison matrix. The element in the matrix means the importance comparison between different threats to the DNS service from a special PoV. This is our next step work and will not be introduced in this paper.

4 Examples

As explained above, we consider all the most important scenarios impacting the normal and secure operation of DNS system. Corresponding to different scenarios, many metrics should be used to assess DNS health. However, considering the impossibility to collect all the necessary information to evaluate the global DNS system, we herein only take "Security" evaluation as an example to illustrate the procedure of our proposed scheme. In this section, we monitor 300 authoritative servers and 500 recursive servers with

[3] In the following, DNS security is chosen as an example to show the process of DNS health evaluation.

some proposed metrics to illustrate the DNS health evaluation procedure. Besides, we analyze the security states of authoritative servers and recursive servers under different threat scenarios to show their health state from the security aspect. Because we cannot subjectively construct the comparison matrix from a special PoV, which depends on the actual environments and requirements, we don't evaluate the overall security states here.

4.1 Case 1

In this case, we mainly focus on the following metrics for the authoritative server:

- DNSSEC supporting
- Server redundancy
- Recursion openness
- Querying latency

For each given metric, the measurement will results in a set of values with different units. Then a necessary step is to normalization. We use real numbers in [0; 1], where 1 is the best value and 0 the worst one. In this way, every measurement can be mapped into a common and uniform mathematical range enabling to aggregate them together. The normalization policies for the above metrics are defined as follows.

DNSSEC supporting. if the monitored server supports DNSSEC, this metric (denoted by D) is set to 1 and it will be set to 0 if not.

Server redundancy. let $S_{\max}$ denote the maximum number of slave servers corresponding to that master server among the monitored servers. Then the quality mapping function $N(S)$: $[0;S_{\max}]\rightarrow[0;1]$ for this metric is defined as

$$N(S)=\frac{S}{S_{\max}} \tag{7}$$

Recursion openness. if the monitored server closes recursion, this metric (denoted by O) is set to 1 and it will be set to 0 if not.

Querying latency. let $Q_{\min}$ denote the minimum value of the querying latency (denoted by Q) among the monitored servers. Then the quality mapping function $N(Q)$: $[Q_{\max};Q_{\min}]\rightarrow[0;1]$ for this metric is defined as

$$N(Q)=\frac{Q_{\min}}{Q} \tag{8}$$

The comparison matrix is constructed as

$$A=\begin{pmatrix} 1 & 7 & 7 & 1 \\ \frac{1}{7} & 1 & 3 & \frac{1}{3} \\ \frac{1}{7} & \frac{1}{3} & 1 & \frac{1}{5} \\ 1 & 3 & 5 & 1 \end{pmatrix} \tag{9}$$

The final weight vector is

$$w=[0.4835,0.1120,0.0559,0.3487] \tag{10}$$

Then the security values of the authoritative servers can be calculated as

$$q=\{D,N(S),O,N(Q)\}\times w^{T} \tag{11}$$

Table 4 shows the evaluation results for the top 10 authoritative servers.

Table 4. Evaluation results of the authoritative server security

	1	2	3	4	5	6	7	8	9	10
D	1	1	1	1	1	1	1	0	0	0
S	3	4	3	3	5	4	2	6	7	5
O	1	1	1	1	0	0	0	0	0	0
Q	0.34s	0.41s	0.53s	0.64s	0.67s	0.71s	0.84s	0.21s	0.24s	0.37s
q	0.8028	0.7820	0.7256	0.7018	0.6728	0.6506	0.6027	0.4447	0.4171	0.2779

4.2 Case 2

In this case, we mainly focus on the following metrics for the recursive server.

- DNSSEC supporting
- Port randomness
- Querying latency

The normalization policies for the above metrics are defined as follows.

DNSSEC supporting. if the monitored server supports DNSSEC, this metric (denoted by D) is set to 1 and it will be set to 0 if not.

Port randomness. let $P_{\max}$ denote the maximum standard deviation of the port randomness value (denoted by P) among the monitored servers. Then the quality mapping function $N(P)$: $[0;P_{\max}]\rightarrow[0;1]$ for this metric is defined as

$$N(P)=\frac{P}{P_{\max}} \tag{12}$$

Querying latency. let $Q_{\min}$ denote the minimum value of the querying latency (denoted by Q) among the monitored servers. Then the quality mapping function $N(Q)$: $[Q_{\max};Q_{\min}]\rightarrow[0;1]$ for this metric is defined as

$$N(Q)=\frac{Q_{\min}}{Q} \tag{13}$$

The comparison matrix is constructed as

$$A=\begin{pmatrix} 1 & 2 & \frac{1}{3} \\ \frac{1}{2} & 1 & \frac{1}{5} \\ 3 & 5 & 1 \end{pmatrix} \tag{14}$$

The final weight vector is

$$w = [0.2297, 0.1220, 0.6483] \quad \textbf{(15)}$$

Then the security values of the recursive servers can be calculated as

$$q = \{D, N(P), N(Q)\} \times w^T \quad \textbf{(16)}$$

Table 5 shows the evaluation results of the top 10 recursive servers.

Table 5. Evaluation results of the recursive server security

	1	2	3	4	5	6	7	8	9	10
D	1	1	1	1	1	1	0	0	0	0
P	30001	24568	25341	19801	21171	17650	14350	14067	13289	13158
Q	0.12s	0.14s	0.28s	0.29s	0.33s	0.35s	0.38s	0.38s	0.39s	0.39s
q	1.0000	0.8853	0.6106	0.5785	0.5515	0.5237	0.2631	0.2619	0.2535	0.2530

5 Conclusion

In order to evaluate the health state of DNS from any possible scenario and PoV, we propose the AHP based method using the basic PoV idea and extended metric sets initially proposed by GCSEC. In which, the AHP is used to set the weights for different metrics according to the special scenario and PoV requirement. Then we construct a platform to monitor the configurations and running states of some authoritative servers and recursive servers. Using the monitoring results, we evaluate their security conditions to illustrate the evaluation process. The results show that our proposed scheme can set the objective weights for the metrics under different scenarios and it can be used by any DNS actors for the service health assessment.

Acknowledgement

The work of J.-H. Lee was supported by Basic Science Research Program through the National Research Foundation of Korea (NRF) funded by the Ministry of Science, ICT & Future Planning (NRF-2017R1A1A1A05001405). The work of G. Geng was supported by the National Natural Science Foundation of China under Grant No. 61375039 and 61272433.

References

[1] P. Mockapetris, *Domain Names– Concepts and Facilities,* IETF RFC 1034, November, 1987.

[2] L. Atzori, A. Iera, G. Morabito, The Internet of Things: A Survey, *Computer Networks*, Vol. 54, No. 15, pp. 2787-2805, October, 2010.

[3] GS1, *Legacy Version*, http://www.gs1.org/epcrfid-epcis-id-keys/epc-frid-architecture-framework/1-7

[4] T-Engine Forum, Ubiquitous ID Center, *Simplified Ucode Resolution Protocol*, October, 2008.

[5] webhosting.info, *Global Statistics*, http://www.webhosting.info/domains-name-statistics

[6] EPCglobal: EPCglobal Object Name Service (ONS) 1.0.1. The EPCglobal Standards Development Process, 2007.

[7] E. Casalicchio, M. Caselli, A. Coletta, Measuring the Global Domain Name System, *IEEE Network*, Vol. 27, No. 1, pp. 25-31, January-February, 2013.

[8] A. Sousa, A. Costa, A. Santos, F. Meneses, M. J. Nicolau, Using DNS to Establish a Localization Service, *Proc. of International Conference on Indoor Positioning and Indoor Navigation*, Busan, Korea, 2014, pp. 385-392.

[9] ICANN, Measuring the Health of the Domain Name System, *Report of the 2nd Annual Global Symposium on DNS Security, Stability, & Resiliency*, Kyoto, Japan, February, 2010.

[10] http://dnseasy.gcsec.org/

[11] http://gcsec.org/

[12] http://conferences.npl.co.uk/satin/

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

[14] R. Arends, R. Austein, M. Larson, D. Massey, S. Rose, *Resource Records for the DNS Security Extensions*, IETF RFC 4034, March, 2005.

[15] R. Arends, R. Austein, M. Larson, D. Massey, S. Rose, *Protocol Modifications for the DNS Security Extensions*, IETF RFC 4035, March, 2005.

[16] S. Castro, D. Wessels, M. Fomenkov, K. Claffy, A Day at the Root of the Internet, *ACM SIGCOMM Computer Communications Review*, Vol. 38, No. 5, pp. 41-46, October, 2008.

[17] R. Liston, S. Srinivasan, E. Zegura, Diversity in DNS Performance Measures, *Proc. of the 2nd ACM SIGCOMM Workshop on Internet Measurement*, Marseille, France, 2002, pp. 19-31.

[18] Y. Sekiya, K. Cho, A. Kato, J. Murai, Research of Method for DNS Performance Measurement and Evaluation Based on Benchmark DNS Servers, *Electronics and Communications in Japan (Part I: Communications)*, Vol. 89, No. 10, pp. 66-75, October, 2006.

[19] Information Technology– Security Techniques-Information Security Risk Management ISO/IEC FIDIS, 27005, 2008.

[20] E. Casalicchio, M. Caselli, D. Conrad, J. Damas, I. N. Fovino, *Reference Architecture, Models and Metrics*, GCSEC Technical document, Version 1.5, July, 2011.

[21] E. Casalicchio, M. Caselli, D. Conrad, J. Damas, I. N. Fovino, *Framework Operation: The Web User Use Case*, GCSEC Report, Version 1.1, July, 2011.

[22] E. Casalicchio, D. Conrad, J. Damas, S. D. Blasi, I. N. Fovino, *DNS Metric Use Cases*, GCSEC Report, Version 1.0, May, 2011.

[23] E. Casalicchio, M. Caselli, A. Coletta, I. N. Fovino, Aggregation of DNS Health Indicators: Issues, Expectations and Results, *Proc. of SATIN 2012*, London, Britain, 2012.

[24] ICANN, *Security, Stability and Resiliency of the Domain Name System*, http://www.gtisc.gatech.edu/pdf/DNSSSRPaper.pdf, January 2009.

[25] A. Hubert, R. van Mook, *Measures for Making DNS More Resilient Against Forged Answers*, IETF RFC 5452, January, 2009.

[26] https://www.icann.org/public-comments/gtld-marketplace-health-2015-11-17-en

[27] T. L. Saaty, *The Analytic Hierarchy Process*, McGraw-Hill, 1980.

[28] S. Fu, H. Zhou, The Information Security Risk Assessment Based on AHP and Fuzzy Comprehensive Evaluation, *Proc. of IEEE 3rd International Conference on Communication Software and Networks*, Xi'an, China, 2011, pp. 124-128.

[29] C. Xu, J. Lin, An Information System Security Evaluation Model Based on AHP and GRAP, *Proc. of International Conference on Web Information Systems and Mining*, Shanghai, China, 2009, pp. 493-496.

[30] T. L. Saaty, Decision Making with the Analytic Hierarchy Process, *International Journal of Services Sciences*, Vol. 1, No. 1, pp. 83-98, January, 2008.

Biographies

Jian Jin is a doctoral candidate at University of Chinese Academy of Sciences. He has been working for China Internet Network Information Center (CNNIC) since 2004 and now is deputy director. As a professor senior engineer of Chinese Academy of Sciences, his research interests include network security and big-data analysis.

Zhiwei Yan received his Ph.D. degree from the National Engineering Laboratory for the Next Generation Internet Interconnection Devices at Beijing Jiaotong University. He joined China Internet Network Information Center in 2011 and is currently an Associate Professor of the Chinese Academy of Sciences. Since April 2013, he has been an Invited Researcher at Waseda University, Japan. His research interests include mobility management and network security.

Jong-Hyouk Lee carried the M.S. and Ph.D. work in Computer Engineering at Sungkyunkwan University, Suwon, Korea. In 2009, he joined the project team IMARA at INRIA, where he undertook the protocol design and implementation for IPv6 vehicular (ITS) communication and security. Dr. Lee started his academic profession at TELECOM Bretagne, France in 2012 as an Assistant Professor. In September of 2013, he moved to Sangmyung University, Cheonan, Korea. He twice received Excellent Research Awards from the School of Information and Communication Engineering, Sungkyunkwan University. Dr. Lee won the Best Paper Award at the *IEEE WiMob 2012* and received the 2015 Best Land Transportation Paper Award from the *IEEE Vehicular Technology Society*. Dr. Lee was a tutorial speaker at the *IEEE WCNC 2013* and *IEEE VTC 2014 Spring*. He is a senior member of the IEEE. He is an associate editor of *Wiley Security and Communication Networks* and *IEEE Transactions on Consumer Electronics*. Research interests include authentication, privacy, and Internet mobility management.

Guanggang Geng received the Ph.D. degree from the State Key Laboratory of Management and Control for Complex Systems, Institute of Automation, Chinese Academy of Sciences, Beijing, China. He was with the Computer Network Information Center, Chinese Academy of Sciences, Beijing, in 2008. He is currently an Associate Professor with the Computer Network Information Center, Chinese Academy of Sciences. His current research interests include machine learning, adversarial information retrieval on the Web, and Web search.