

# An approach to prevention to the DNS Injection attacks on the base of system level comparison method MM

Michał Melaniuk  
Military University of Technology  
ul. Kaliskiego 2,  
00-908 Warszawa, Poland  
Email: [michal.melaniuk@wat.edu.pl](mailto:michal.melaniuk@wat.edu.pl)

**Abstract**—This article describes the use of the comparison method MM to protect the Internet user from the effects of DNS Injection attacks. A description of the basic concepts of this area of the computer network and the dangers of DNS Injection attacks is presented. The description of the MM method used in the literature is concluded. In the paper the concept of using above-mentioned method to protect Internet user from the effects of DNS Injection attacks and the initial design of the DNS server software including the diagnostic component are presented.

## I. INTRODUCTION

Domain Name System (DNS) is one of the most commonly used service over the Internet. It allows, among others, to connect to a web site using its mnemonic name (usually easier to remember) instead of its IP address. Converting a domain name to an IP address is done by a DNS server that, in most cases, is a separate host in the network. The DNS user does not have direct control over the server, which involves the risk of obtaining an incorrect name mapping from the server. Unfortunately, practice shows that there is a lack of universal way by which the user can make sure that the responses received from the DNS servers are reliable. Correct DNS performance is critical to the smooth operation and security of the Internet. The lack of entries in the DNS server records database may cause the network resources to be inaccessible, while erroneous entries may redirect network traffic to the incorrect location specified (and controlled) by the attacker [3].

This article focuses on protecting the Internet user from the effects of DNS Injection attacks – which relies on modification of the entries in the DNS server mapping tables [9]. Any Internet user who will be able to send false updates to the DNS server or detect and be able to exploit the vulnerabilities in the server software could be an attacker. Unlike traditional security systems (like firewalls, IDS/IPS), the proposed method is to detect the effects of an attack (not to protect against it).

## II. RELATED WORK

The proposed approach of protecting the Internet user against the effects of DNS Injection attacks attempts to use a comparative method known as the MM<sup>1</sup> method [6], [7]. In the literature there are works that use this method most often to diagnose a network of processors (with different logical structure). A. Arciuch in [1] presented the technical aspects of diagnosing a network of microprocessors with a mild type of degradation using the MM method, R. Kulesza and Z. Zieliński in [4] used this method to determine diagnostic insight of network of processors. A. Sengupta and A. T. Dahbura in [8] proposed usage of the MM method in a self-diagnosing multiprocessor system, and G.Y. Chang, G.H. Chen and G.J. Chang in [2] used the MM<sup>\*2</sup> model to develop a sequential diagnosis of the processor network.

In this work it was decided to use a different approach and use the comparison method to diagnose DNS servers.

## III. PROPOSAL

This section is based on [4] and [5]. The MM method uses comparative graph as a way to represent the logical structure of nodes with the corresponding set of comparative tests. This concept (along with examples) is explained later in this article. In the area of the problem (mutual testing of DNS servers) an elementary comparative test will be sending by a comparator a DNS query to resolve a domain name to both nodes of a comparative pair. Then the comparator verifies that the obtained results - IP addresses - are identical. These type of checks will be performed periodically, every  $k^3$  queries, ensuring continuous DNS servers reliability without overloading the network.

A *fit* comparator will give the opinion that a comparative pair is fit (the result of comparative test will be equal to 0) if the results of the DNS query are identical. The different

<sup>1</sup>The name of the method comes from the names of the creators: M. Malek and J. Maeng.

<sup>2</sup>The MM\* model is characterized by the use of diagnostic structures consisting of all possible comparative tests, while the MM model uses a minimal number of comparative tests to detect  $t$  damaged network nodes.

<sup>3</sup> $k$  is an arbitrary value.

results of the DNS query will result in an opinion that the comparison pair is *unfit* (the result of the comparative test will be equal to 1), with at least one node from the comparative pair is compromised (it is not indicated which one). The opinion expressed by a suitable comparator is consistent with reality. An unfit comparator gives an opinion that is random and assumes a value of 0 or 1.

#### A. Significant features of the MM type comparative structure

Consider an exemplary logical structure of a network described by a connected common graph  $G=(E, U)$ . An example graph is shown in Fig. 1.

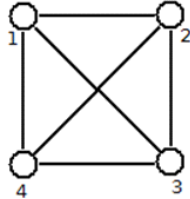


Fig 1. Sample graph representing the logical structure of network

The logical structure  $G$  corresponds to the set of all comparative tests denoted by  $\Psi(G)$ , and the single comparative test is denoted by  $\psi \in \Psi'$ ,  $\Psi' \subseteq \Psi(G)$ . For comparison test  $\psi$  exists a set of comparators labeled  $K(\psi)$  and a set of comparative pairs labeled  $P(\psi)$ . The set of nodes involved in the comparative test  $\psi$  is labeled  $E(\psi)$ . A single comparative test is shown in Fig. 2.

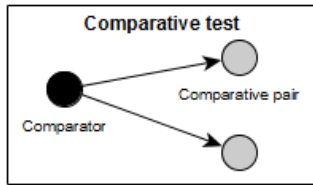


Fig 2. Illustration of single comparative test

In a comparative test the comparator  $e_k \in E(G)$  orders the comparative pair  $e_i, e_j \in E(G)$  the same task and checks if the results are identical.

The comparative test is denoted by  $(e_k; e_i, e_j)$ . The result of the comparative test  $d((e_k; e_i, e_j))$  is equal to:

$$d((e_k; e_i, e_j)) = \begin{cases} 0 & \text{for } [n(e_k)=0 \wedge r(e_i|e_k)=r(e_j|e_k)] & \text{case a)} \\ 1 & \text{for } [n(e_k) \wedge r(e_i|e_k) \neq r(e_j|e_k)] & \text{case b)} \\ x \in \{0,1\} & \text{for } n(e_k)=1 & \text{case c)} \end{cases} \quad (1)$$

where  $n(e_k)$  is functional reliability of node  $e_k$  and  $r(e_j|e_k)$  is the result of a task ordered by node  $e_k$  and executed by node  $e_j$ .

In the area of the problem in *case c)*, unlike the classic MM model, the unfitness of the DNS server that is the comparator has no impact on the outcome of the test it performs. During the comparison, the comparator verifies the mutual compatibility of the results obtained from the nodes

of the comparative pair. These results are not matched with the entries of the DNS server records database, so even if it had been compromised (as a result of a DNS Injection attack), name mappings in its database would not affect the accuracy of the opinion. The interpretation of diagnosis results is presented in Table I.

TABLE I.  
THE DIAGNOSIS RESULTS INTERPRETATION IN PROPOSED METHOD

$n(e_k)$	$n(e_i)$	$n(e_j)$	$d((e_k; e_i, e_j))$
x	0	0	0
	0	1	1
	1	0	1
	1	1	1

**Definition 1.** [10] The computer network described by the structure  $G$  is defined as *single-step  $t$ -diagnosable* by a set of comparative tests  $\Psi' \subseteq \Psi(G)$ , if each pair of sets  $E'$  and  $E''$  of unfit nodes such that  $|E'| \leq t$  and  $|E''| \leq t$  is distinguishable by at least one comparative test  $\psi \in \Psi'$ .

**Definition 2.** [10] *Comparative graph* of computer network described by the structure  $G$  for a set of comparative tests  $\Psi' \subseteq \Psi(G)$ , is called such ordinary graph  $\hat{G}(G, \Psi') = (E(G), U(G, \Psi'))$  with labeled edges that  $[(e', e'') \in U(G, \Psi')] \leftrightarrow [\exists_{\psi \in \Psi'} : P(\psi) = \{e', e''\}]$ , where the label of the  $(e', e'')$  edge is  $K(\psi)$ .

**Property 1.** [4], [6] The necessary condition for graph  $G$  to be  $t$ -diagnosable by the set of comparative tests  $\Psi' \subseteq \Psi(G)$  is to fulfill the dependence:

$$(|E(G)| \geq \max\{t+3, 2 \cdot t+1\}) \wedge (\forall_{e \in E(G)} : \mu(e) \geq t) \quad (2)$$

where  $\mu(e)$  denotes the input degree of the node  $e$ .

**Property 2.** [6] The structure is  $t$ -diagnosable by the comparative tests  $\Psi' \subseteq \Psi(G)$  if and only if for every pair of subsets of nodes  $E_1, E_2 \subseteq E(G)$  such that  $E_1 \neq E_2$  and  $|E_1| = |E_2| = t$  one of the following conditions is true:

$$\text{a) } \exists_{\psi', \psi'' \in \Psi(G)} : \left[ (K(\psi'), K(\psi'')) \cap (E_1 \cup E_2) = \emptyset \wedge \left( |P(\psi') \cap (E_1 \setminus E_2)| = 1 \vee |P(\psi'') \cap (E_2 \setminus E_1)| = 1 \right) \right] \quad (3)$$

$$\text{b) } \exists_{\psi' \in \Psi(G)} : \left[ |P(\psi') \cap (E_1 \setminus E_2)| = 2 \wedge |P(\psi') \cap (E_1 \cup E_2)| = \emptyset \right] \quad (4)$$

$$\text{c) } \exists_{\psi' \in \Psi(G)} : \left[ |P(\psi') \cap (E_2 \setminus E_1)| = 2 \wedge |P(\psi') \cap (E_1 \cup E_2)| = \emptyset \right] \quad (5)$$

#### B. Method of identifying unfit servers

The results of the comparative tests conducted in one diagnostic session will create so-called *the global syndrome*. Each server has in its resources reference values determining the reliability of servers participating in performed diagnostic session using the indicated diagnostic structure. These reference values are different for each diagnostic structure and are defined as *the pattern of syndromes*. The example of the pattern of syndromes for diagnostic structure presented later in Fig. 5. is presented in Table II. Single

value (row in example Table II) is often defined as *pattern syndrome*<sup>4</sup>.

TABLE II.  
THE EXAMPLE OF THE PATTERN OF SYNDROMES

$i$					1	2	3	4	5	6	7	8
$K(\psi_i)$					1	1	2	2	3	3	4	4
$P(\psi_i)$					2	2	3	3	4	4	1	1
					4	3	1	4	2	1	3	2
$e$	1	2	3	4	$d(\psi_i)$							
$n(e)$												
	0	0	0	0	0	0	0	0	0	0	0	0
	0	0	0	1	1	0	0	1	1	1	0	0
	0	0	1	0	0	1	1	1	0	0	1	0
	0	1	0	0	1	1	0	0	1	0	0	1
	1	0	0	0	0	0	1	0	0	1	1	1

Each server after building the global syndrome will attempt to match it to one of the pattern syndromes. After a positive match, it will be possible to indicate the reliability status of the tested DNS servers.

C. Requirements for the developed method

An unauthorized change of even one record in the DNS server records database creates a threat to users which are communicating with the node whose entry was modified. Such conclusion can be derived on the basis of the analysis of the impact of attacks described, among others in [9].

It is required that the method will be able to detect a specified number of compromised DNS servers in the network environment (defined as  $t$ ). The mechanism of action consists in mutual testing of DNS servers by sending the response to the DNS query. The number of required comparisons depends on the number of unfit nodes to be detected. The collected responses will be evaluated, which will allow to determine which of them are invalid and indirectly to make it possible to indicate the unfit DNS servers.

The article focuses on the prevention and protection of the user against the considered type of attacks. The results of the comparisons that are sent to the client computer will allow him to use only those DNS servers that have been identified as fit. It is assumed that the developed method will be able to detect DNS servers successfully exploited by DNS Injection.

The diagnostic software that would use the developed method would extend the DNS server architecture. Working in the background, it would regularly examine the suitability of DNS servers while informing the DNS client about the results of the tests. The preliminary scheme of the DNS server diagnostics software is shown in Fig. 3. It is assumed that the software will carry out two main tasks:

- sending DNS queries for indicated domain and receiving replies,
- group replies and base on them conclude the reliability of DNS servers participating in the test.

The initial class scheme of the DNS server after adding the diagnostic module is shown in Fig. 4.

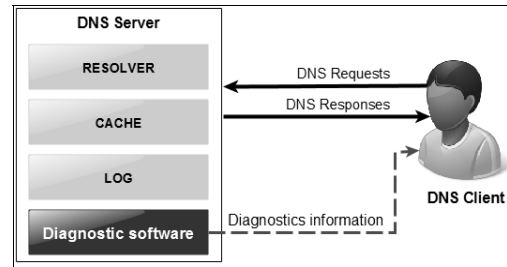


Fig 3. Architecture diagram of the DNS servers diagnostics software

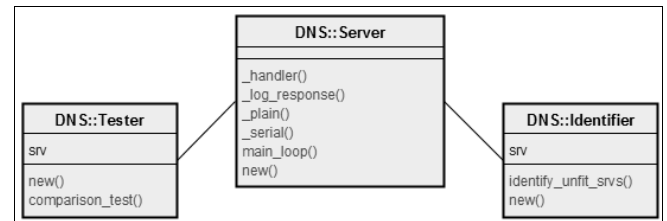


Fig 4. Initial Class scheme of the DNS servers diagnostics software

D. Description of the developed method

The proposal of protecting the Internet user, developed within this article, is supposed to fulfill the requirements mentioned in sections B. and C.. In addition, the following assumptions must be met.

1. The comparative test consists of three DNS servers: one being a comparator (denoted as  $K(\psi)$ ), the other being a comparative pair (denoted as  $P(\psi)$ ).
2. Comparing the response pairs from the DNS servers to the DNS query sent by the comparator will be understood as a *test*.

The logical structure of the network of tested nodes can be described by connected common graph  $G=(E, U)$ . The developed method of protecting the Internet user is based on the  $t$ -diagnosable (by comparison set  $\Psi' \subseteq \Psi(G)$ ) comparative graph  $\hat{G}(G, \Psi')$  which fulfills the necessary and sufficient conditions for the MM method (dependences (2)-(5) presented in section A.). These dependencies guarantee a suitable comparative graph as a diagnostic structure. Except for the number of nodes participating in the comparison and the appropriate number of comparisons completed (which is forced by the Property 1 described in section A.), mentioned comparisons must involve the appropriate nodes to determine the fitness of the DNS servers (which is forced by the Property 2 described in section A.).

From the Definition 1 of the  $t$ -diagnosable MM structure it follows that if each of the nodes has  $t$  comparative tests with different nodes and is judged by different comparators, then

<sup>4</sup>The notions: *the global syndrome*, *pattern syndrome* and *the pattern of syndromes* are well defined in [4].

such structure is  $t$ -diagnosable. Thus, it is possible to propose a comparative graph for the graphical structure shown in Fig. 1, represented by the graph  $\hat{G}(G, \Psi')$  shown in Fig. 5.

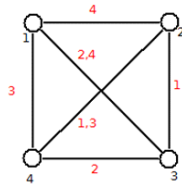


Fig 5. Comparative graph  $\hat{G}(G, \Psi')$  corresponding to the optimal diagnostic structure  $(G, \Psi')$

The node in the graph  $\hat{G}(G, \Psi')$  corresponds to the DNS server. From the set of comparative tests  $\Psi'$  the individual comparative tests  $\psi_i$  ( $i \in \{1, 2, \dots, |\Psi'|\}$ ) are designated. The algorithm for diagnosing network of DNS servers (implemented by each server) is shown below in the pseudocode<sup>5</sup>.

```

for each  $\psi_i \in \Psi'$  do
  if  $server = K(\psi_i)$ 
    Send to  $P(\psi_i)$ : DNS query for host "xyz";
    Collect responses from  $P(\psi_i)$ ;
     $d(\psi_i) := \text{Result of comparison responses from } P(\psi_i)$ ;
  do
     $TMP\_Global\_Syndrome[\psi_i] := d(\psi_i)$ ;
    Send  $TMP\_Global\_Syndrome$  to all DNS servers in diagnostic structure;
  else Send to  $K(\psi_i)$ : Response to DNS query for host "xyz" from  $K(\psi_i)$ ;
end
Collect  $TMP\_Global\_Syndrome$  from all servers;
Build  $Global\_Syndrome$ ;
Decode  $Global\_Syndrome$  and identify which server is unfit;
Send  $List\_of\_unfit\_servers$  to client;

```

The DNS server which is the comparator in the  $i$  test (denoted by  $K(\psi_i)$ ) sends to the nodes of the comparative pair (denoted by  $P(\psi_i)$ ) the DNS query for the domain name for example: *wat.edu.pl*. Servers of the comparison pair answers with the IP address which they have stored in their records databases. Next the comparator compares the responses according to the dependence (1) and the result of the comparative test (denoted by  $d(\psi_i)$ ) is passed to each DNS server. All comparative tests form diagnostic structure are performed as described. Then, on the basis of the results of the tests, identification of unfit nodes takes place according to identification method described in section B.. The end user is informed which DNS servers were indicated as unfit - a so-called *black list of DNS servers* is created which are not used for resolving domain names. As a result, the user only uses the servers that are diagnosed as fit it means that those which can be trusted.

#### IV. SUMMARY

This article proposes a method of protecting the Internet user from the effects of DNS Injection attacks. The proposed

method uses the comparative tests - MM model. Based on the diagnostic structure described by comparative graph, comparative tests are carried out involving three nodes (DNS servers). One is a comparator and the other two are comparative pair. The results of the comparative tests are complemented by DNS servers and unfit nodes are indicated based on the mentioned results. The user is given a list (in for example DNS TXT record) of unfit (untrusted) servers that he or she should not use to resolve domain names. The developed solution can be customized for use in a DNS client environment who itself (as a reliable core) will compare the results from the DNS servers and determine which nodes are unfit.

A number of laboratory experiments were performed in order to confirm the effectiveness of the developed method. In a prepared computer network with suitable number of DNS servers correctness of the method was verified. Servers were "attacked" in random order, resulting the invalid responses to the DNS queries. Then, in such prepared lab environment, diagnostic software implementing proposed method was executed. The obtained results were comparable with the actual state of the laboratory network, which allows me to conclude about the practical application of the developed method. The obtained results provide the basis for developing a more accurate test environment and conducting a series of experiments for example including checking whether the network topology affects the diagnostic results.

#### REFERENCES

- [1] A. Arciuch, "Techniczne aspekty diagnozowania sieci procesorów o łagodnej degradacji typu sześcian 4-wymiarowy metodą prób porównawczych", *Przegląd Teleinformatyczny nr 2*, 2013
- [2] G.Y. Chang, G.H. Chen, G. J. Chang, "(t,k) – Diagnosis for Matching Coposition Networks under the MM\* Model", *IEEE Trans. Comput.*, 2007, 56, 1, s. 73-79.
- [3] T. Grabowski, "DNS spoofing, czyli podszywanie się pod serwer DNS", *Hakin9*, no. 1. Available at: [http://www.centrum.bezpieczenstwa.pl/artykuly/h9\\_dns.pdf](http://www.centrum.bezpieczenstwa.pl/artykuly/h9_dns.pdf)
- [4] R. Kulesza, Z. Zieliński, "Wnikliwość diagnozowania sieci procesorów metodą porównawczą". In: *Systemy czasu rzeczywistego. Postępy badań i zastosowania*. Red. Z. Zieliński, WKŁ, Warszawa, 2009, s. 211-225. (in Polish)
- [5] R. Kulesza, Z. Zieliński, "Diagnosis resolution of processors' network using the comparison method", *PRZEGLĄD ELEKTROTECHNICZNY (Electrical Review)*, vol. 89, No 9, 2010, p. 157-162.
- [6] J. Maeng, M. Malek, "A Comparison Connection Assignment for Self-Diagnosis of Multiprocessor Systems", *Digest Int. I Symp. FTC*, 1981, 173-175.
- [7] M. Malek, "A Comparison Connection Assignment for Diagnosis of Multiprocessor Systems", *Proc. Seventh Int'l Symp. Computer Architecture*, 1980, 31-35.
- [8] A. Sengupta, A. T. Dahbura, "On self-diagnosable multiprocessor systems: Diagnosis by the comparison approach", *IEEE Trans. Comput.*, vol. 41, 11, 1992, p.1386-1396.
- [9] Sparks, Neo, Tank, Smith, Dozer, "The Collateral Damage of Internet Censorship by DNS Injection", *SIGCOMM Computer Communication Review* 42.3, 2012
- [10] Ł. Strzelecki, "Metody projektowania ekonomicznych  $t$ -diagnostowalnych struktur diagnostyki systemowej dla sieci procesorów typu binarnego sześcianu 4-wymiarowego", Ph.D., WAT WCY, 2012

<sup>5</sup>The example value *xyz* shown in pseudocode could be any hostname, for example: *wat.edu.pl*.