PRZEGLĄD TELEINFORMATYCZNY
NR 3-4, 2018

Badanie możliwości wykorzystania metody porównawczej do zapobiegania skutkom ataków typu DNS Injection

Michał MELANIUK

Instytut Teleinformatyki i Automatyki, WCY, WAT,
ul. Gen. Witolda Urbanowicza 2, 00-908 Warszawa
michal.melaniuk@wat.edu.pl

STRESZCZENIE: W artykule przedstawiono zagadnienie wykorzystania metody porównawczej do zapobiegania skutkom ataków typu DNS Injection. Zaproponowano rozwiązanie wykorzystujące przedmiotową metodę oraz opisano opracowane środowisko laboratoryjne do eksperymentalnego zbadania skuteczności działania opracowanego rozwiązania.

SŁOWA KLUCZOWE: metoda MM, metoda prób porównawczych, diagnostyka, serwer DNS, DNS Injection

1. Wprowadzenie

Jedną z najczęściej wykorzystywanych usług dostępnych w sieci Internet jest usługa Systemu Nazw Domenowych (DNS, ang. *Domain Name System*). Dzięki wspomnianej usłudze możliwe jest przede wszystkim nawiązanie połączenia z wybraną stroną internetową wykorzystując jej nazwę mnemoniczną (zazwyczaj łatwiejszą do zapamiętania) zamiast jej adresu IP. W większości przypadków przekształcenia nazw na adresy IP (lub odwrotnie) dokonywane są przez osobny węzeł sieci nazywany serwerem DNS, jednakże zdarza się, że taki serwer pracuje również lokalnie na danym hoście. Użytkownik systemu DNS nie ma bezpośredniej kontroli nad serwerem, co wiąże się z ryzykiem uzyskania od serwera niepoprawnego odwzorowania nazwy. Niestety praktyka pokazuje, że brakuje uniwersalnego sposobu, za pomocą którego użytkownik mógłby upewnić

się, że odpowiedzi otrzymane od serwerów DNS są wiarygodne. Brak wpisów w bazie rekordów DNS może spowodować brak dostępu do zasobów konkretnej sieci, natomiast błędne wpisy mogą przekierować ruch sieciowy do wskazanej przez atakującego, niepoprawnej lokalizacji będącej pod jego kontrolą. Zatem można stwierdzić, że poprawne działanie systemu DNS jest krytyczne dla sprawnego działania i bezpieczeństwa sieci Internet. [3]. Postanowiono zbadać możliwość opracowania sposobu minimalizacji lub całkowitego zapobiegania skutkom ataków względem serwerów DNS. Jako podstawę wybrano metody diagnostyki systemowej. Niniejsze opracowanie stanowi materiał wstępny do porównania skuteczności zastosowania różnych metod diagnostyki systemowej w przedmiotowym obszarze. W niniejszej pracy skupiono się na metodzie prób porównawczych celem zbadania jakości jej zastosowania w wykrywaniu skutków ataków typu *DNS Injection*.

W niniejszym artykule skupiono się na ochronie użytkownika sieci Internet przed skutkami ataków typu *DNS Injection* – polegających na modyfikacji wpisów w tablicach odwzorowań serwera DNS [14]. Każdy użytkownik sieci Internet, który będzie w stanie znaleźć i wykorzystać luki bezpieczeństwa w oprogramowaniu serwera DNS, bądź wysłać do niego odpowiednio sfałszowane aktualizacje wpisów w tablicach odwzorowań może być atakującym. Opisywana metoda ma na celu wykrywanie skutków ataku DNS Injection, a nie ochrony przed nim, jak to czynią tradycyjne systemy bezpieczeństwa (takie jak IDS/IPS lub zapory sieciowe). W obszarze zagrożeń związanych z atakami typu *DNS Injection* znaleźć można prace, m.in. [5], [20], [22] jednakże prezentują one zupełnie odmienne podejście do tematu ochrony użytkownika przed tego typu zagrożeniami niż omawiane w niniejszym opracowaniu. W [5] autorzy przeprowadzili badania serwerów DNS z różnych obszarów sieci Internet pod kątem oceny ich podatności na ataki *DNS Cache Injection*. Na podstawie przeprowadzonych prac badacze stwierdzili, że ponad 90% z testowanych serwerów DNS było podatnych na realizowane ataki, co oznacza, że ich konfiguracja może być ukradkiem regularnie modyfikowana. Prezentowane metody nadużyć dodatkowo nie wymagają istotnych nakładów pracy podczas realizacji ataków. W pracy [20] opisano system REMeDy, który w sposób automatyczny ocenia spójność odpowiedzi serwerów DNS w danej sieci. Prezentowany system poprzez pasywne nasłuchiwanie ruchu sieciowego pozwala wykryć dodane do sieci węzły, które kierują ruch sieciowy do niepoprawnych lokalizacji lub zainfekowane serwery DNS. System bazuje na wskazaniach serwerów DNS dostawcy usług internetowych (ang. *Internet Service Provider – ISP*) i zakłada, że są one zawsze poprawne. Opracowanie [22] prezentuje rozwiązanie T-DNS – system DNS oparty na protokole TCP. Zastosowanie komunikacji połączeniowej pozwoliło na ograniczenie: możliwości podszywania się pod inne serwery DNS, realizacji ataków DoS typu *Amplification*. Dodatkowo

prezentowany system wykorzystuje szyfrowanie transmisji przy użyciu mechanizmu TLS.

2. Powiązane prace

Opracowana *metoda ochrony użytkownika sieci Internet przed skutkami ataków typu DNS Injection*[1] zakłada wykorzystanie metody prób porównawczych określanej mianem metody MM[2] [9]. W literaturze znaleźć można prace, w których wykorzystywano wspomnianą metodę najczęściej do diagnozowania sieci procesorów (o różnej strukturze logicznej). A. Arciuch w [1] zaprezentował techniczne aspekty diagnozowania sieci procesorów o łagodnej degradacji metodą MM. Autor w swojej pracy zaimplementował wspomnianą metodę w fizycznej sieci zbudowanej z wykorzystaniem mikrokomputerów Micro2440. Opracowana sieć pracuje w określony sposób przeplatając seanse diagnostyczne (w których następuje weryfikacja poprawnej pracy wszystkich węzłów sieci) okresami roboczymi (w których sieć wykonuje swoje zadania). R. Kulesza i Z. Zieliński w [5] wykorzystali wspomnianą metodę do określania wnikliwości diagnostycznej sieci procesorów. Autorzy w swoim opracowaniu określili reguły, które pozwalają jednolite definiowanie klas sieci procesorów o określonych własnościach diagnostycznych. Na podstawie opracowanych reguł możliwe jest wytworzenie automatu programowego, który będzie określał własności diagnostyczne sieci bazując na wzorcach syndromów. A. Sengupta i A. T. Dahbura w [13] zaproponowali wykorzystanie metody MM w samo-diagnozującym się systemie z wykorzystaniem modelu MM we wspomnianym systemie. W pracy podany został zestaw kryteriów określających czy wadliwe procesory systemu mogą zostać wykryte na podstawie przeprowadzonych porównań wykonywanych przez nie zadań. Ponadto w pracy zaproponowany został algorytm wielomianowy realizujący zadanie identyfikacji uszkodzonych jednostek. G.Y. Chang, G.H. Chen i G.J. Chang w [2] wykorzystali model *MM**[3] do opracowania sekwencyjnego diagnozowania sieci procesorów. W podejściu tym wymagane jest określenie odpowiedniej liczby procesorów niezdatnych i ich naprawienie w każdej iteracji algorytmu. W pracy opisano algorytm, który zastosowano do diagnostyki m.in. sieci typu hipersześcian. Ponadto dostępnych

[1] W celu uproszczenia w dalszej części artykułu określana w skrócie jako *Metoda*.

[2] Nazwa metody pochodzi od nazwisk twórców: M. Malek oraz J. Maeng.

[3] Model MM* charakteryzuje się wykorzystaniem struktur diagnostycznych składających się ze wszystkich możliwych prób porównawczych, podczas, gdy model MM wykorzystuje minimalną liczbę prób porównawczych, która zapewnia detekcję *t* uszkodzonych węzłów sieci.

jest wiele interesujących prac opisujących różne zastosowania metod diagnostyki systemowej, m.in.: [3], [9]-[12]. Jianxi Fan w [3] badał możliwość zastosowania metody prób porównawczych do wykrywania niezdatnych węzłów w sieci o strukturze pochodnej hipersześcianu określonej mianem *crossed cube*. Autor wykazał, że taka *n*-wymiarowa struktura jest *n*-diagnozowalna dla $n \geq 4$, podczas gdy dla hipersześcianu ta zależność zachodzi dla $n \geq 5$. W [9] autorzy rozważali wykorzystanie diagnostyki adaptacyjnej, która dąży do zmniejszenia liczby rund testowych i samych testów, za pomocą modelu MM dla struktur typu hipersześcian *n*-wymiarowy. Wykazana została możliwość diagnozowania *n*-wymiarowych hipersześcianów w opisany sposób w ograniczonej liczbie testów. Przykładowo, dla $n \geq 5$ przedstawiona metoda potrzebuje co najwyżej 6 rund testowych i $2^n + 2n^3 + 8n^2$ testów do wykrycia *n* uszkodzonych węzłów. Jiarong Liang i Qian Zhang w [10] opracowali metodę *t/s*-diagnozowania sieci o strukturze hipersześcianu z wykorzystaniem m.in. metody prób porównawczych. W pracy zaprezentowano teoretyczne zagadnienia związane z *t/s*-diagnozowalnością oraz przedstawiono algorytm izolowania uszkodzonych węzłów w podzbiory. Natomiast w pracy [12] autorzy rozważają zagadnienie warunkowej diagnozowalności systemu, w którym pojawiają się uszkodzone węzły. W pracy skupiono się na strukturze sieci określanej mianem *Split-Star*, która diagnozowana jest z wykorzystaniem modelu PMC[4].

W niniejszej pracy postanowiono wykorzystać inne podejście i zastosować metodę prób porównawczych w diagnozowaniu poprawności działania serwerów DNS.

3. Proponowane rozwiązanie

Niniejszy punkt powstał w oparciu o [5] i [8]. Metoda MM wykorzystuje graf porównań jako jeden ze sposobów reprezentacji struktury logicznej węzłów wraz z odpowiadającym jej zbiorem prób porównawczych. Pojęcie grafu porównań (wraz z przykładami) zostało wyjaśnione w dalszej części niniejszego artykułu. W omawianym obszarze problemu, który stanowi wzajemne testowanie się serwerów DNS, jako elementarny test porównawczy rozumiane jest wysłanie przez komparator identycznego zapytania rozwinięcia nazwy domenowej do obu węzłów stanowiących parę porównawczą. Następnie zadaniem komparatora jest zweryfikowanie, że uzyskane adresy IP (odpowiedzi na wysłane zapytania) są identyczne. Opisany rodzaj sprawdzeń będzie wykonywany okresowo, co

[4] Dodatkowe referencje związane z modelem PMC zawarto w punkcie 5.

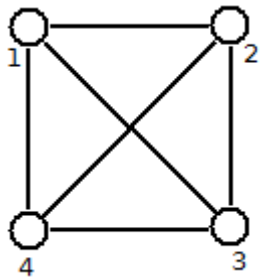
k[5] zapytań zapewniając ciągłą niezawodność serwerów DNS bez nadmiernego obciążania sieci komputerowej.

Jako węzeł *zdatny* rozumiany jest serwer DNS, który w sposób poprawny odwzorowuje nazwę domenową na adres IP (zwracany adres IP prowadzi do właściwej lokalizacji). Węzeł *niezdatny* jest to serwer DNS, którego odwzorowania nazw na adresy IP są niepoprawne (zwracany adres IP prowadzi do niewłaściwej lokalizacji, np. kontrolowanej przez agresora). *Uszkodzenie* jest to zainfekowanie serwera DNS, w wyniku którego zwraca on niewłaściwe adresy IP.

Zdatny komparator zaopiniuje, że para porównawcza jest zdatna (wynik testu porównawczego przyjmie wartość 0), jeżeli wyniki złożonych zapytań DNS są identyczne. Różne wyniki testu skutkują zaopiniowaniem o niezdatności pary porównawczej (wynik testu porównawczego przyjmie wartość 1), przy czym niezdatny jest przynajmniej jeden węzeł z pary porównawczej (nie jest wskazane który). Opinia wyrażona przez zdatny komparator jest więc zgodna ze stanem faktycznym. Niezdatny komparator (w założeniach metody MM) wyraża opinię, która jest przypadkowa i przyjmuje wartość 0 lub 1.

3.1. Istotne cechy struktury porównawczej typu MM

Rozpatrzmy przykładową strukturę logiczną sieci opisaną spójnym grafem zwykłym $G = \langle E, U \rangle$. Przykładowy graf przedstawiono na rysunku 1.



Rys. 1. Przykładowy graf reprezentujący strukturę logiczną

Strukturze logicznej G odpowiada zbiór wszystkich prób porównawczych oznaczony poprzez $\Psi(G)$, a pojedynczą próbę porównawczą oznaczono symbolem $\psi \in \Psi'$, $\Psi' \subseteq \Psi(G)$. Dla próby porównawczej ψ istnieje zbiór komparatorów oznaczany jako $K(\psi)$ oraz zbiór par porównawczych oznaczony

[5] Wartość parametru *k* jest dowolna.

jako $P(\psi)$. Zbiór węzłów biorących udział w próbie porównawczej ψ oznaczono jako $E(\psi)$.

W próbie porównawczej węzeł $e_k \in E(G)$ będący komparatorem zleca parze porównawczej $\{e_i, e_j\} \subset E(G)$ jednakowe zadanie, a następnie sprawdza, czy uzyskane wyniki są identyczne.

Próbę porównawczą oznacza się poprzez $(e_k; e_i, e_j)$. Wynik próby porównawczej $d\left((e_k; e_i, e_j)\right)$ może przyjąć jedną z trzech wartości (zależną od stanów niezawodnościowych komparatora i pary porównawczej):

$$d\left((e_k; e_i, e_j)\right) = \begin{cases} 0\ dla\ [e_k = 0 \wedge r(e_i|e_k) = r(e_j|e_k)] & przyp.a) \\ 1\ dla\ [e_k = 0 \wedge r(e_i|e_k) \neq r(e_j|e_k)] & przyp.b) \\ x \in \{0,1\}\ dla\ e_k = 1 & przyp.c) \end{cases} \quad (1)$$

gdzie $n(e_k)$ jest funkcjonalna niezawodnością węzła e_k oraz $r(e|e_k)$ jest wynikiem zadania zleconego przez węzeł e_k, a wykonanego przez węzeł e.

W rozważanej dziedzinie problemu (wzajemne testowanie się serwerów DNS) w $przyp.c)$ niezdatność serwera DNS będącego komparatorem nie ma wpływu na wynik realizowanego przez niego testu. Podczas porównania komparator weryfikuje wzajemną zgodność wyników otrzymanych od węzłów pary porównawczej. Wyniki te nie są zestawiane z wpisami posiadanymi przez dany serwer DNS dlatego nawet jeśli posiadałby on skompromitowane (w wyniku ataku *DNS Injection*) odwzorowania nazw w swojej bazie nie wpłyną one na poprawność opiniowania. Interpretacja wyników próby porównawczej została przedstawiona w tabeli 1. Natomiast $przyp.a)$ i $przyp.b)$ mają zastosowanie zgodnie z powyższym wzorem.

Tab. 1. Interpretacja wyników próby porównawczej w opracowanej *Metodzie*

$n(e_k)$	$n(e_i)$	$n(e_j)$	$d\left((e_k; e_i, e_j)\right)$
1	0	0	0
	0	1	1
	1	0	1
	1	1	1

Określenie 1. [15] Sieć komputerów opisana strukturą G określa się jako *jednokrokowo t-diagnozowalną*[6] *za pomocą zbioru prób porównawczych* $\Psi' \subseteq \Psi(G)$, jeżeli każda para zbiorów E' i E'' niezdatnych węzłów takich, że $|E'| \leq t$ i $|E''| \leq t$, jest rozróżnialna za pomocą choć jednej próby porównawczej $\psi \in \Psi'$.

Określenie 2. [15] *Grafem porównań* sieci komputerów o strukturze G dla zbiorów prób porównawczych $\Psi' \subseteq \Psi(G)$ nazywamy taki graf zwykły $\hat{G}(G, \Psi') = \langle E(G), U(G, \Psi') \rangle$ o opisanych krawędziach, że $[(e', e'') \in U(G, \Psi')] \leftrightarrow \left[\exists_{\psi \in \Psi'} : P(\psi) = \{e', e''\}\right]$, gdzie etykietą krawędzi (e', e'') jest $K(\psi)$.

Własność 1. [5], [9] Warunkiem koniecznym, aby graf G był t-diagnozowalny za pomocą zbioru prób porównawczych $\Psi' \subseteq \Psi(G)$ jest spełnienie zależności:

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

gdzie $\mu(e)$ oznacza stopień wejściowy węzła e.

Własność 2. [9] Graf G jest t–diagnozowalny za pomocą prób porównawczych $\Psi' \subseteq \Psi(G)$, wtedy i tylko wtedy, gdy dla każdej pary podzbiorów węzłów $E_1, E_2 \subseteq E(G)$ takich, że $E_1 \neq E_2$ oraz $|E_1| = |E_2| = t$, spełniony jest jeden z poniższych warunków:

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

b) $$\exists_{\psi' \in \Psi(G)} : [|P(\psi') \cap \{E_1 \backslash E_2\}| = 2] \wedge [K(\psi') \cap \{E_1 \cup E_2\} = \emptyset] \tag{4}$$

c) $$\exists_{\psi' \in \Psi(G)} : [|P(\psi') \cap \{E_2 \backslash E_1\}| = 2] \wedge [K(\psi') \cap \{E_1 \cup E_2\} = \emptyset] \tag{5}$$

3.2. Metoda identyfikowania niezdatnych serwerów

Wyniki testów porównawczych przeprowadzonych w ramach jednej sesji diagnostycznej utworzą tzw. *syndrom globalny*. Każdy serwer posiada w swoich zasobach wartości wzorcowe określające niezawodność poszczególnych węzłów w wykorzystywanej strukturze. Wspomniane wartości wzorcowe są różne dla różnych struktur porównawczych i są określane mianem *wzorca syndromów*.

[6] Jako *t*-diagnozowalność rozumiana jest możliwość wskazania maksymalnie *t* uszkodzonych węzłów w sieci. Przykładowo struktura *3*-diagnozowalna umożliwia wskazanie maksymalnie trzech uszkodzonych węzłów. Opisano to dokładnie w dalszej części artykułu.

Przykład wzorca syndromów dla struktury diagnostycznej zaprezentowanej w dalszej części artykułu na rysunku numer 3 przedstawiono w tabeli numer 2. Pojedyncza wartość (wiersz w tabeli numer 2) jest często określana mianem *syndromu wzorcowego*[7].

Tab. 2. Przykładowy wzorzec *syndromów*

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

Każdy serwer DNS po uzyskaniu wyników poszczególnych prób porównawczych od innych węzłów tworzy syndrom globalny (zawierający wyniki wszystkich przeprowadzonych prób porównawczych). Następnie próbuje dopasować otrzymany syndrom do jednego z syndromów wzorcowych w posiadanym wzorcu syndromów dla danej struktury diagnostycznej. Uzyskanie dopasowania pozwala określić stany niezawodnościowe serwerów DNS biorących udział w sesji diagnostycznej.

3.3. Wymagania względem opracowanej *Metody*

Na podstawie analizy wyników ataków względem serwerów DNS, które zrealizowano m.in w [14] można stwierdzić, że istotne jest zapewnienie integralności zapisów w bazie odwzorowań serwera DNS. Nieautoryzowana zmiana choćby jednego rekordu we wspomnianej bazie odwzorowań serwera stanowi zagrożenie dla użytkowników, którzy się z nim komunikują i może

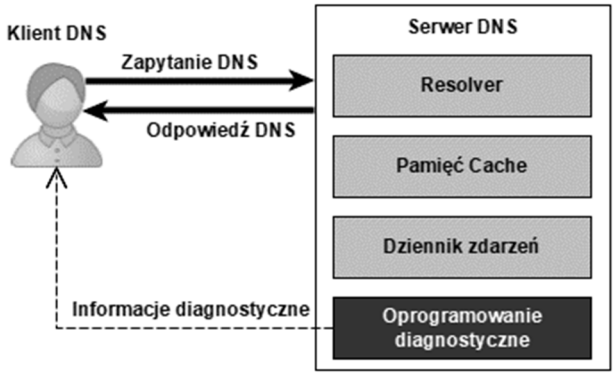
[7] Pojęcia: *syndrom globalny, syndrom wzorcowy* i *wzorzec syndromów* zostały dokładnie zdefiniowane w [5].

skutkować przekierowaniem ruchu sieciowego do nieprawidłowej (często kontrolowanej przez agresora) lokalizacji.

Założono, że opracowana *Metoda* ma umożliwiać wykrycie określonej liczby skompromitowanych serwerów DNS w środowisku sieciowym (wspomniana liczba jest zdefiniowana jako t). Mechanizm działania polega na wzajemnym testowaniu się serwerów DNS poprzez wysłanie odpowiedzi na zapytanie DNS. Liczba wymaganych porównań zależy od liczby uszkodzonych węzłów do wykrycia. Zebrane odpowiedzi zostaną porównane, co pozwoli określić, które z nich są błędne i pośrednio, aby umożliwić wskazanie niezdatnych serwerów DNS.

Artykuł koncentruje się na ochronie użytkownika przed omawianym typem ataków i zapobieganiu jego skutkom. Wyniki działania *Metody* wysyłane do komputera klienckiego pozwolą mu używać tylko tych serwerów DNS, które zostały zidentyfikowane jako zdatne. Zakłada się, że opracowana *Metoda* będzie w stanie wykryć serwery DNS zaatakowane przez agresora z wykorzystaniem DNS Injection.

Oprogramowanie diagnostyczne, które wykorzystuje opracowaną *Metodę*, rozszerza architekturę serwera DNS. Działając w tle, regularnie sprawdza zdatność serwerów DNS. Ponadto na żądanie informuje klienta DNS o wynikach testów. Uproszczony schemat oprogramowania do diagnostyki serwerów DNS przedstawiono na rysunku 2.



Rys. 2. Uproszczony schemat oprogramowania diagnostycznego

Oprogramowanie diagnostyczne wykonuje trzy główne zadania:

- wysyłanie zapytań DNS dla wskazanej nazwy domenowej i odbieranie odpowiedzi,
- grupowanie odpowiedzi i na ich podstawie określenie niezawodność serwerów DNS uczestniczących w teście,
- przekazanie klientowi informacji o zdatności serwerów DNS.

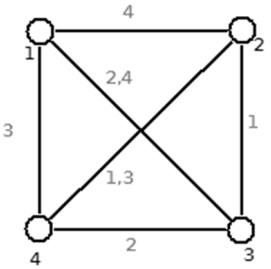
3.4. Opis opracowanej *Metody*

Proponowana w ramach niniejszego artykułu *Metoda* spełnia wymagania przytoczone w punktach 3.2 - 3.3. Ponadto spełnione są następujące założenia:

- porównanie odpowiedzi na zapytania DNS pochodzące z dwóch serwerów DNS rozumiane jest jako *test porównawczy*,
- w teście porównawczym biorą udział trzy serwery DNS: komparator (oznaczany jako $K(\psi_i)$) oraz dwa serwery stanowiące parę porównawczą (oznaczane jako $P(\psi_i)$).

Logiczną strukturę sieci testowanych węzłów opisać można spójnym grafem zwykłym $\mathrm{G} = \langle \mathrm{E}, \mathrm{U} \rangle$. Opracowana *Metoda* bazuje na *t*-diagnozowalnym (za pomocą zbioru prób porównawczych $\Psi' \subseteq \Psi(\mathrm{G})$) grafie porównań $\widehat{\mathrm{G}}(\mathrm{G}, \Psi')$, który spełniać musi warunki konieczne i wystarczające dla metody MM (zależności (2) – (5) przedstawione w punkcie 3.1). Te zależności gwarantują, że graf porównań jest odpowiednią strukturą diagnostyczną. Poza odpowiednią liczbą węzłów biorących udział w porównaniu i odpowiednią liczbą porównań (wymuszoną przez właściwość 1 opisaną w punkcie 3.1), wspomniane porównania muszą angażować odpowiednie węzły do określenia zdatności serwerów DNS (co wymuszone przez właściwość 2 opisaną w punkcie 3.1).

Dla przykładowej struktury logicznej zaprezentowanej wcześniej na rysunku 1 można zaproponować strukturę porównawczą daną grafem porównań $\widehat{\mathrm{G}}(\mathrm{G}, \Psi')$ zaprezentowanym na rysunku 3.



Rys. 3. Graf porównań $\widehat{G}\langle G, \Psi' \rangle$ odpowiadający optymalnej strukturze diagnozowania $\langle G, \Psi' \rangle$

Węzeł w grafie $\widehat{G}\langle G, \Psi' \rangle$ odpowiada serwerowi DNS. Ze zbioru prób porównawczych Ψ' wyznaczane są poszczególne próby porównawcze ψ_i ($i \in \{1,2, \dots, |\Psi'|\}$). Dla każdej wyznaczonej próby porównawczej realizowane są wymienione poniżej operacje.

1. Serwer DNS będący komparatorem próby i wysyła do pary porównawczej zapytanie DNS o rozwinięcie nazwy hosta, np. *host1.mm.pl*.

2. Serwery pary porównawczej odpowiadają adresem IP hosta, który posiadają zapisany w swoich bazach odwzorowań.
3. Komparator porównuje otrzymane adresy IP zgodnie z zależnością (1), a otrzymany wynik porównania zapisuje w syndromie globalnym i przekazuje do pozostałych serwerów DNS w strukturze.

Następnie na podstawie zebranych wyników ze wszystkich prób porównawczych w sesji diagnostycznej serwery DNS identyfikują niezdatne węzły zgodnie z metodą opisaną w punkcie 3.2. Użytkownik końcowy może pozyskać listę niezdatnych serwerów DNS, które tworzą tzw. *czarną listę serwerów DNS*. Użytkownik końcowy nie powinien korzystać z usługi DNS serwerów znajdujących się na *czarnej liście*. Wynikowo użytkownik korzysta jedynie z serwerów zdiagnozowanych jako zdatne, czyli takie, którym można zaufać.

4. Badanie skuteczności opracowanej metody

4.1. Opis środowiska laboratoryjnego

W celu praktycznej weryfikacji skuteczności opracowanej *Metody* zbudowano odpowiednie środowisko laboratoryjne. Wykorzystano rozwiązania wirtualizacji, które pozwalają na wygodne i szybkie zarządzanie serwerami DNS pracującymi w środowisku. Na chwilę obecną środowisku działa 7 serwerów DNS, co pozwala na wykorzystywanie maksymalnie *3*-diagnozowalnej struktury porównawczej.

Wszystkie serwery zostały zainstalowane jako maszyny wirtualne w ramach wirtualizatora vmWare ESXi 6.5.0 i pracują pod kontrolą systemu operacyjnego Linux Debian 4.9. Maszynom wirtualnym przydzielono po jednym wirtualnym procesorze, 400MB pamięci operacyjnej oraz 2GB przestrzeni dyskowej. Usługa serwera DNS realizowana jest przy pomocy oprogramowania BIND9.

Odnośnie konfiguracji DNS przyjęto, że każdy serwer będzie posiadał rolę tzw. *mastera* i będzie obsługiwał domenę *mm.pl*. Istotnym z punktu widzenia badań przydatności opracowanej *Metody* będzie wpis w konfiguracji DNS dotyczący hosta *host1.mm.pl*, którego poprawny adres IP to *192.168.206.201*.

4.1.1. Wykorzystywane struktury porównawcze

W literaturze przedstawione są prace opisujące algorytmy i sposoby generowania odpowiednich struktur *t*-diagnozowalnych zarówno dla wykorzystywanej metody porównawczej, jak i innych metod diagnostyki systemowej. Przykładowo Ł. Strzelecki w swoich publikacjach opisuje możliwości wykorzystywania do realizacji przedmiotowego zadania metodę adaptacyjną [15], [19] lub algorytm genetyczny [17], [18]. Na potrzeby opracowanego środowiska laboratoryjnego wykorzystano struktury *1*, *2* i *3*-diagnozowalne wygenerowane z wykorzystaniem algorytmu opisanego w [15].

Każdy serwer DNS w środowisku laboratoryjnym przechowuje w swoich zasobach wygenerowane struktury porównawcze w formie tabeli, analogicznej względem przedstawionej tabeli numer 2. Struktury są wykorzystywane przy określaniu konkretnych testów do realizacji przez dany serwer.

4.1.2. Opracowane oprogramowanie

Na potrzeby środowiska laboratoryjnego opracowano programy realizujące następujące operacje:

- infekowanie serwerów DNS,
- wielokrotne powtarzanie sesji diagnostycznych,
- testowanie zdatności środowiska laboratoryjnego opracowaną *Metodą*.

Oprogramowanie infekujące ma za zadanie podmienić konfigurację serwera DNS na niepoprawną. Zmianie podlega adres IP dotyczący hosta *host1.mm.pl*. Oprogramowanie generuje w sposób pseudolosowy błędny adres IP, który zostanie umieszczony w konfiguracji serwera w momencie infekcji. Dodatkowo oprogramowanie wykorzystywane jest do naprawiania serwerów DNS po skończonym teście poprzez podmianę niepoprawnego adresu IP na właściwy dla hosta.

Oprogramowanie testujące ma za zadanie wskazać niezdatne serwery DNS przy pomocy opracowanej *Metody*. Następnie uzyskane wskazanie jest porównywane z rzeczywistym stanem sieci serwerów i na tej podstawie określana jest poprawność działania *Metody*. Dodatkowo oprogramowanie testujące pozwala na realizację badań w dwóch wariantach:

- infekowanie kilku serwerów DNS tym samym błędnym adresem IP,
- infekowanie kilku serwerów DNS różnymi błędnymi adresami IP.

4.2. Wyniki zrealizowanych badań

W środowisku laboratoryjnym opisanym w punkcie 4.1 przeprowadzono badania skuteczności opracowanej *Metody* w wykrywaniu skompromitowanych serwerów DNS. Procedura badań była następująca:

1) przeprowadzenie badań dla *1*, *2* i *3*-diagnostycznych struktur porównawczych – serwery były infekowane różnymi niepoprawnymi adresami IP,
2) przeprowadzenie badań dla *1*, *2* i *3*-diagnostycznych struktur porównawczych – serwery były infekowane identycznymi niepoprawnymi adresami IP.

Powyższa procedura została zrealizowana 1000 razy, by na podstawie uzyskanych wyników możliwe było wyciągnięcie miarodajnych wniosków. Podczas badań zbierano następujące statystyki: skuteczność wskazania niezdatnych serwerów oraz średni, minimalny i maksymalny czas trwania pojedynczej sesji diagnostycznej.

Poniżej w tabeli numer 3 przedstawiono zestawienie uzyskanych wyników. Rozpatrywano łącznie 5 różnych przypadków:

- P1 – struktura *1*-diagnozowalna (w tym przypadku nie ma rozróżnienia na infekowanie tymi samymi lub różnymi adresami IP, bo infekowany jest tylko 1 węzeł),
- P2 – struktura *2*-diagozowalna, każdy serwer infekowany innym adresem IP,
- P3 – struktura *2*-diagozowalna, każdy serwer infekowany tym samym adresem IP,
- P4 – struktura *3*-diagozowalna, każdy serwer infekowany innym adresem IP,
- P5 – struktura *3*-diagozowalna, każdy serwer infekowany tym samym adresem IP.

Po każdej iteracji serwery DNS są przywracane do pierwotnego (zdatnego) stanu. Przy dużym obciążeniu środowiska (wykonywanie testów co kilka sekund) zdarzały się przypadki, że jeden z serwerów w teście *n* posiadał jeszcze ustawienia z testu *n-1* – serwer nie zdążył wczytać aktualnej konfiguracji zanim został odpytany o adres IP w teście *n*. W takich przypadkach otrzymywano błędne wyniki, które nie były brane pod uwagę w określaniu skuteczności *Metody*.

Tab. 3. Wyniki przeprowadzonych pomiarów

Przypadek	Skuteczność [%]	Czas średni [s]	Czas minimalny [s]	Czas maksymalny [s]
P1	100	0,817	0,724	7,522
P2	100	1,581	1,394	12,534
P3	0	1,531	1,394	12,534
P4	100	2,945	2,767	8,053
P5	0	4,235	2,665	16,916

4.3. Wnioski

Na podstawie wyników badań przedstawionych w punkcie 4.2 można stwierdzić, że zaproponowana metoda jest w stanie zidentyfikować niezdatne serwery w przypadku, gdy zostaną zainfekowane różnymi błędnymi adresami IP lub, gdy mamy do czynienia z jednym infekowanym serwerem. W opisywanych przypadkach (P1, P2 i P4) skuteczność metody wyniosła 100%. Metoda bez problemu jest w stanie wskazać zaatakowane serwery, gdy te odpowiadają różnymi błędnymi adresami IP.

Jednocześnie można stwierdzić, że w przypadkach zainfekowania kilku serwerów tym samym błędnym adresem IP (przypadki P3 i P5) proponowana metoda nie jest w stanie wskazać niezdatnych serwerów. Zaistniała sytuacja wynika z faktu, że przy porównywaniu odpowiedzi od dwóch zainfekowanych serwerów oba uzyskane adresy IP są takie same (ale oba przekierują użytkownika do niepoprawnej lokalizacji kontrolowanej przez agresora) przez co wynik porównania wskazuje brak różnic i metoda stwierdza, że para porównawcza jest zdatna (niezgodnie ze stanem faktycznym).

Bardzo ważną obserwacją jest fakt, że w przypadku infekcji kilku serwerów tym samym błędnym adresem IP wynikiem metody jest informacja o braku dopasowania syndromu globalnego do wzorca. Oznacza to, że metoda nie jest w stanie wskazać uszkodzonych serwerów i nie zwraca żadnych wyników. W związku z tym, nie występuje w proponowanej metodzie błąd polegający na wskazaniu w rzeczywistości zdatnych serwerów, jako niezdatne.

Dodatkowo można zaobserwować, że skuteczność metody nie zależy od *t*-diagnozowalności struktury. W związku z tym zwiększanie jej złożoności jest zasadne tylko w przypadku, gdy chcemy mieć możliwość wykrycia większej liczby serwerów. Opisywana sytuacja może mieć miejsce w przypadku, gdy jakaś organizacja uzna (np. na podstawie analizy ryzyka), że wymagane jest, aby mieć

możliwość wykrycia większej liczby serwerów – ryzyko infekcji np. 5. serwerów jest nieakceptowalne i fakt takiego nadużycia powinno się dać wykryć.

Ponieważ metoda porównawcza nie sprawdziła się w każdym z analizowanych przypadków dobrym pomysłem wydaje się być sprawdzenie przydatności innych metod diagnostyki systemowej. W ramach dalszych prac planuje się rozbudowanie środowiska laboratoryjnego o możliwość wykorzystania np. metody PMC [6], [9], [10] [20] lub BGM [6], [10]. W podanej literaturze zostały szczegółowo opisane własności metod PMC i BGM oraz występujące między nimi zależności i sposoby zastosowania w praktyce.

Odnośnie czasów realizacji sesji diagnostycznych, zaobserwować można ich liniowy wzrost wraz ze wzrostem *t*-diagnozowalności struktury, co jest zachowaniem poprawnym. Obserwowana sytuacja pozwala wnioskować, że dla wyższych *t* czas realizacji pojedynczego testu będzie rósł proporcjonalnie do złożoności struktury. Zasadnym jest natomiast podjęcie działań, których celem będzie optymalizacja pracy algorytmu i w efekcie skrócenie czasu wykonania pojedynczej sesji diagnostycznej.

5. Podsumowanie

Celem artykułu było przedstawienie środowiska laboratoryjnego do eksperymentalnego badania możliwości zastosowania metody porównawczej do wykrywania zainfekowanych serwerów DNS. Realizacja przedmiotowego zadania wymagała zbudowania środowiska komputerowego, w którym działać będzie określona liczba serwerów DNS oraz opracowania oprogramowania, którego zadaniem było odpowiednie infekowanie i naprawianie wspomnianych serwerów. Ponadto wymagane było opracowanie aplikacji do realizacji wielokrotnych badań środowiska z wykorzystaniem zaproponowanej *Metody*. Opis środowiska laboratoryjnego przedstawiono w punkcie 4.1 natomiast zaproponowane rozwiązanie opisano w punkcie 3.

Przeprowadzone testy empiryczne (dla dużej liczby przypadków) wykazują jedynie połowiczną skuteczność proponowanego rozwiązania. Metoda porównawcza znakomicie radzi sobie z detekcją serwerów DNS zainfekowanych różnymi błędnymi adresami IP. Niestety jednocześnie wykrywanie serwerów zainfekowanych tymi samymi adresami IP nie jest możliwe. Z tego względu wymagane są dalsze badania w kierunku zwiększenia skuteczności proponowanego rozwiązania, np. poprzez weryfikację możliwości zastosowania w przedmiotowym obszarze metody PMC lub BGM.

Literatura

[1] ARCIUCH A., *Techniczne aspekty diagnozowania sieci procesorów o łagodnej degradacji typu sześcian 4-wymiarowy metodą prób porównawczych*. Przegląd Teleinformatyczny 2013, nr 2, s. 3-11.

[2] CHANG G.Y., CHEN G.H., CHANG G.J., *(t,k) – Diagnosis for Matching Composition Networks under the MM* Model*. IEEE Transactions Computers, 2007, 56, 1, pp. 73-79.

[3] FAN J., *Diagnosability of crossed cubes under the comparison diagnosis model*. IEEE Transactions on Parallel and Distributed Systems, 2002, vol. 13, 10, pp. 687-692.

[4] GRABOWSKI T., *DNS spoofing, czyli podszywanie się pod serwer DNS*. Hakin9, nr 1, http://www.centrum.bezpieczenstwa.pl/artykuly/h9_dns.pdf (Dostęp 22.04.2015 r.).

[5] KLEIN A. SHULMAN H. WAIDNER M., *Internet-Wide Study of DNS Cache Injections.* IEEE INFOCOM 2017 – IEEE Conference on Computer Communications, 2017, pp. 1-9.

[6] KULESZA R., *Podstawy diagnostyki sieci logicznych i komputerowych.* Wyd. II, Warszawa: ITA WAT, 2000.

[7] KULESZA R., ZIELIŃSKI Z., *Wnikliwość diagnozowania sieci procesorów metodą porównawczą*. Systemy czasu rzeczywistego. Postępy badań i zastosowania. Red. Z. Zieliński, WKŁ, Warszawa, 2009, s. 211-225.

[8] KULESZA R., ZIELIŃSKI Z., *Diagnosis resolution of processors' network using the comparison method*. Przegląd Elektrotechniczny (Electrical Review), 2010, vol. 89, Nr 9, s. 157-162.

[9] LAI PL., *Adaptive system-level diagnosis for hypercube multiprocessors using a comparison model.* Journal Information Sciences—Informatics and Computer Science, Intelligent Systems, Applications: An International Journal, 2013, vol. 252, pp. 118-131.

[10] LIANG JR., FENG H., DU X., *Intermittent Fault Diagnosability of Interconnection Networks*. Journal of Computer Science and Technology, 2017, vol. 32, no 6, pp. 1279-1287.

[11] LIANG J., ZHANG Q., *The t/s – Diagnosability of Hypercube Networks Under the PMC and Comparison Models*. IEEE Access, 2017, vol. 5, pp. 5340 – 5346.

[12] LIN L.M., XU L., ZHOU S.M., *Conditional diagnosability and strong diagnosability of Split-Star Networks under the PMC model*. Journal Theoretical Computer Science, 2015, vol: 562, issue C, pp. 565-580.

[13] SENGUPTA A., DAHBURA A.T., *On self-diagnosable multiprocessor systems: Diagnosis by the comparison approach.* IEEE Transactions on Computers, 1992, vol. 41, 11, pp. 1386-1396.

[14] SPARKS, NEO, TANK, SMITH, DOZER, *The Collateral Damage of Internet Censorship by DNS Injection.* Newsletter ACM SIGCOMM Computer Communication Review, 2012, vol. 42, issue 3, pp.21-27.

[15] STRZELECKI Ł., RENCZEWSKI K., *Adaptacyjna metoda wyznaczania ekonomicznych m-diagnozowalnych struktur opiniowania diagnostycznego typu PMC*. Biuletyn ITA, 2008, nr 25, s. 139-153.

[16] STRZELECKI Ł., *Metody projektowania ekonomicznych t-diagnozowalnych struktur diagnostyki systemowej dla sieci procesorów typu binarnego sześcianu 4-wymiarowego*. Rozprawa doktorska, WAT, WCY, Warszawa, 2012.

[17] STRZELECKI Ł., ZIELIŃSKI Z., *Projektowanie struktur opiniowania diagnostycznego z wykorzystaniem algorytmu genetycznego*. Biuletyn ITA, 2009, nr 27, s. 19-31.

[18] STRZELECKI Ł., *Wyznaczanie struktur diagnozowania porównawczego przy wykorzystaniu algorytmu genetycznego*. Przegląd Teleinformatyczny, 2016, nr 3-4, s. 19-30.

[19] STRZELECKI Ł., *Wyznaczanie struktur diagnozowania porównawczego z użyciem metody PSO*. Przegląd Teleinformatyczny, 2017, nr 1-2, s. 3-12.

[20] TREVISAN M., DRAGO I., MELLIA M., MUNAFO M.M., *Automatic Detection of DNS Manipulations*. IEEE International Conference on Big Data, 2017, pp. 4010-4015.

[21] WANG R., ZHU Q., *The h-extra conditional diagnosability of burnt pancake networks under the PMC model*. 2017 First International Conference on Electronics Instrumentation & Information Systems (EIIS), 2017, pp. 1-6.

[22] ZHU L., HU Z., HEIDEMANN J., WESSELS D., MANKIN A., SOMAIYA N., *Connection-Oriented DNS to Improve Privacy and Security*. Proceedings of the 2015 IEEE Symposium on Security and Privacy, 2015, pp. 171-186.

Exploring the possibility of using a comparative method to prevent effects of DNS Injection attacks

ABSTRACT: The article presents the problem of using the comparative method to prevent effects of DNS Injection attacks. A solution based on the presented method was proposed, and a developed laboratory environment was described for experimental examination of the effectiveness of the developed solution.

KEYWORDS: MM method, Malek Maeng model, comparative method, diagnostics, DNS server, DNS Injection

Praca wpłynęła do redakcji: 2.07.2018 r.