Information Sciences 479 (2019) 593–606

Contents lists available at ScienceDirect

Information Sciences

journal homepage: www.elsevier.com/locate/ins

Smart collaborative distribution for privacy enhancement in moving target defense

Fei Song[a], Yu-Tong Zhou[b], Yu Wang[c], Tian-Ming Zhao[a], Ilsun You[d,*], Hong-Ke Zhang[a]

[a] School of Electronic and Information Engineering, Beijing Jiaotong University, PR China
[b] Institute of Education and Economy Research, University of International Business and Economics, PR China
[c] School of International Trade and Economics, University of International Business and Economics, PR China
[d] Department of Information Security Engineering, Soonchunhyang University, Republic of Korea

ARTICLE INFO

Article history:
Received 18 August 2017
Revised 28 May 2018
Accepted 3 June 2018
Available online 6 June 2018

Keywords:
Moving target defense
Smart collaboration
Network privacy
DNS attacks
Port hopping

ABSTRACT

The Moving Target Defense (MTD) has been widely discussed in many communities to upgrade the network reliability, survivability, dependability, etc. However, utilizing MTD in privacy protection still needs more investigations. In this paper, we propose a smart collaborative distribution scheme to enhance the privacy based on MTD guidelines. A target application scenario is the Domain Name System (DNS) that is experiencing serious and complex privacy issues. The preliminary and potential risks are firstly analyzed based on DNS attack approaches, DNS server locations and the vulnerability of user privacy. Then, the details of our scheme are illustrated through port number assignment patterns, main procedures of dynamic port hopping and the implementation method. To quantitatively evaluate the performance, an analytical model was established from theoretical perspectives. The relationships between multiple parameters and overall system capacity are explored as well. The validation results demonstrate that the smart collaborative distribution is able to improve the privacy without affecting the basic DNS functionality.

1. Introduction

The privacy issue has been widely recognized as one of the most critical issues in computer networks. The Internet not only brings the pervasive and free entrances for users, but also provides convenient and inexpensive opportunities for attackers. Nowadays, many information leakage incidents, i.e. typical privacy issues, have been reported and discussed frequently all over the world [31]. A possible reason is more data will trigger more potential safety hazard. When the volume of content is continually extended, the original leakage ratio should be drastically reduced to maintain the balance. Although the researchers attempt to find a tradeoff solution between personal information protection and effective network usage, it is still a tough problem with lots of uncertainty. Traditional definitions have clearly delimitated the range of this field, however, such partition is gradually blurred since more novel paradigms (cloud computing, fog computing, edge computing) are emerging. Our society has been warned that the appropriate schemes are urgently needed [15].

The Moving Target Defense (MTD) [22,32], as a set of promising mechanisms, has been noticed by academic experts and industrial practitioners. Here, we only choose two representative cases from the layered network architecture. For the

* Corresponding author.
E-mail address: isyou@sch.ac.kr (I. You).

https://doi.org/10.1016/j.ins.2018.06.002
0020-0255/

bottom layers, the primitive practice could be traced back to pulling and plugging the wired cable to different slots in Local Area Network (LAN). The advantage is that the physical isolation can be enabled. However, such manual port hopping will be complicated when the network scale is large. To improve the scalability, Virtual LAN (VLAN) and Virtual Extensible LAN (VxLAN) are proposed to achieve the similar functionalities. Multiple subnets can be established and reconstructed based on service requirements. Both manual and automatic port hopping are supported to accomplish the logical isolation. For the upper layers, a tentative implementation was using fixed destination port number and random source port number in Transmission Control Protocol (TCP), User Datagram Protocol (UDP) and other transport protocols. Although the original design intention may not be for privacy enhancement, it indeed inspired many creative followers. The applications of Peer to Peer (P2P), Virtual Private Network (VPN), social network, etc., utilize dynamic port hopping scheme to avoid the blocking and control of the Internet Service Provider (ISP), which protects the user privacy indirectly. Since current Domain Name System (DNS) [7,17] is qualified to leverage the benefits of MTD as well, we would like to focus on this specific field.

The DNS is well known as a high level proxy between users and machines to swap the Uniform Resource Locator (URL) for Internet Protocol (IP) addresses. The former and latter are familiar to the human and computers, respectively. When the requests generated by the users are correctly received, iterative or recursive DNS lookup will be initiated immediately. Generally, The DNS servers in LAN should record several frequently-used or famous URLs to avoid unnecessary inquiring. If no appropriate DNS items are matched, the requests will be transmitted to the other DNS servers directly (will be detailed in Section 2). Finally, zero, one or more IP addresses might be returned based on the inquiring results. Even though the extensive usages of such procedures are acceptable, many significant problems are still calling for better solutions [6,16]. For instance, port 53 has been occupied by TCP and UDP for DNS packets transmission, which provides an open window for attackers to monitor such fixed target. By utilizing the characteristics of MTD, such embarrassed situation can be relieved.

The motivation of this paper is to propose a smart collaborative distribution scheme to enhance the privacy when DNS lookup is executed. The target is to achieve dynamic port allocation and hopping during the relevant DNS workflow. Several significant questions should be fully considered during the operation process: How does the DNS maintain the wiretap difficulty based on affordable cost? What are the core elements of new procedure design? How does the administrator of DNS investigate the overall performance of the novel scheme via mathematical perspective? We will attempt to answer them in the following Sections.

The contribution of this paper is classified into two parts: (1) A smart collaborative distribution scheme is proposed based on MTD and the essential of implementation is also discussed. (2) A comprehensive system model is presented based on Markov theory and mathematical analysis is introduced to evaluate the results quantitatively.

The structure of this paper is: In Section 2, the preliminary and potential risks are provided. The characteristics of multiple DNS attack approaches are summarized and primary locations of DNS servers are presented. Then, four different privacy leakage cases are analyzed. In Section 3, the design details of the smart collaborative distribution are introduced. Current assignment schemes of port number are reviewed. Two algorithms are proposed based on the requirements of the end host and DNS server. The implementation results are abstracted from prototype system. Relevant modifications inside DNS packets are also illustrated. In Section 4, the analytical model is established to quantitatively validate the performance. Different scenarios are selected to analyze the relationships among multiple parameters. In Sections 5 and 6, the related work and conclusions are given, respectively.

2. Preliminary and potential risks

From the perspective of the network, with the high speed development of social software, lots of random, unreadable and ephemeral URLs are created and propagated, which inevitably lead to longer latency for DNS lookup process. Massive DNS requests sent by mobile terminals, fix terminals, Internet of Thing (IoT) devices, etc. will further increase the burdens. Although there are 13 root servers and plentiful mirror servers, the scalability and dependability of the DNS should be reconsidered to handle these emerging challenges [9,29,37]. From the perspective of the end host, the balance between simplicity guarantee and privacy protection is always a hot topic. For realizing the efficient DNS lookup, the designer has put the simplification at the first place. It is a sophisticated strategy when multiple factors exist simultaneously. However, such philosophy also leaves more space for the hackers to eavesdrop the DNS lookup processes. By monitoring the public TCP or UDP port number, they could easily learn the details and launch different kinds of attacks. In Internet Engineering Task Force (IETF), there are several relevant working groups, such as DNS Private Exchange (dprive), Domain Name System Operations (dnsop).

In previous discussions, only one aspect was pointed out. However, there are still more underlying threatens during the DNS packet transmission [38]. To better learn and analyze the overall procedures, we simply summarize a list of multiple DNS attacks by focusing on the user privacy. Both the locations of primary DNS servers and the influences of content leakage are introduced as well.

2.1. Attack approaches for DNS

In the process of DNS lookup and feedback, there are dozens of attack methods [18–20], which increase the difficulty of system protection. For example, by caching the intermediate information, sniffing attack may be accomplished without disturbing or affecting the regular data transmission. By inserting the virus or Trojan code into original program, injection

attack may break or watch the operation procedures. By pretending the ordinary behaviors of the end host, capture attack may exchange forged packets with the server. By simulating the normal actions of the remote server, phishing attack may send the wrong results back to the end host. By occupying the available bandwidth, resource attack may create large quantities of flows and deliver them to the server from different sources. By requesting the similar services, repetition attack may exhaust the server and seriously decrease the performance. All these approaches could be utilized to obtain the user privacy in DNS environment. In this paper, we select some of them as the main defending targets in following analysis.

2.2. Primary DNS server locations

To demonstrate the operations of DNS lookup, we suppose that an IP address is just assigned to one URL by the authority. Then, the necessary steps of inquiring will be: (1) The end host examines the default mapping information locally (like "hosts" file in Window OS). (2) The end host may generate a request and transmit it to the primary DNS server. (3) The primary DNS server may generate a request and transmit it to other DNS servers. (4) The location (i.e. the IP address) of the top level DNS server could be returned back. (5) The primary DNS server may generate a request and transmit it to such specific location. (6) The repetitive actions could be executed to find other level DNS servers before the correct IP address of the target is achieved. (7) The primary DNS server should send the results to the initiator.

The importance of the primary DNS server is obvious. According to the popular implementation, the potential deployment places could be: (1) Inside LAN: The company, institution, organization, even individual user could establish a DNS server. In such case, the latency between the primary DNS server and the end host will be quite small. (2) Inside ISP: different servers could be built through anycast and various improvements can be achieved to decrease the Round Trip Time (RTT) of DNS lookup. (3) Inside Wide Area Network (WAN): Many IP addresses (like 114.114.115.115, 8.8.4.4, etc.) are opened to the public for providing DNS functionalities. However, the users need to agree with the privacy policy before using, which means their personal information might be collected passively.

It is no doubt that higher wiretap possibilities could be witnessed if more network equipment (routers, switches, etc.) are added between the primary DNS server and the end host. Such circumstance will not be changed when following DNS lookup are involved. Here, we would like to focus on the first situation and present a smart collaborative distribution scheme to solve it.

2.3. The vulnerability of user privacy

If the attack approaches have been successfully launched during the DNS lookup process, the influences related with user privacy will appear via different patterns.

First, it is simple to observe that the main URL of website can be captured by supervising the DNS packets. Several prefix identifiers (such as "news.qq.com", "movie.youku.com", "auction.jd.com") will further reveal the potential interest of the user. Moreover, the basic classifications (such as current location, browsing mode, native language) also carry the specific characteristics. All these primitive information is sufficient to describe a generic profile.

Second, the adequate information may still be obtained even though the full content of the webpage was not transmitted to the DNS server directly. For instance, if the end host would like to browse:

tudou.com/58416457/72154869/66132479,

the content before the first slash (i.e. "tudou.com") will be exchanged for query. When the IP address has been obtained correctly from DNS, the end host will transmit the remainders to the website immediately. It seems that the supervision on DNS cannot directly intercept the specific webpage. Nevertheless, a number of strange DNS lookup may be initiated by the prewritten inline code, which creates the special "fingerprint" for different webpages. One main reason of these strange DNS lookup is for statistics purpose. By adding the templates of statistic companies, such as

umeng.com, baifendian.com, statcounter.com, shinystat.com,

the visit volume, distribution and other properties can be easily achieved, which is significant for website construction and optimization. The "fingerprint" of a webpage can be summarized by recording the URLs, request sequence, request frequency, etc. When a specific webpage is confirmed based on data mining, the full link of the user can be obtained.

Third, the privacy may be threatened even if the user did not browse any websites. When the end host accesses the Internet, the application and operating system are able to initiate multiple DNS lookup automatically. For example, IOS, Linux and Windows may ask for "upgrade" URLs; Safari, Firefox and IE browsers may initiate default "home page" URLs; Software installed inside portable devices can push "advertisement" URLs. Such DNS lookup could expose sensitive information (like kernel version, service type, etc.), which should be observed carefully.

Fourth, comprehensive analysis can be adopted by attackers for high level prediction. We only demonstrate two representative examples here. (1) Identity verification. If the website browsing habits of a particular person have been stored in detail, the data set of usages could be established expediently. Then, the identity can be verified even though the user is not using the same equipment or browser to access the Internet. (2) Identity classification. If a user has visited several relevant URLs during a short period, the possible relations of these websites and the category of the user could be estimated. Assuming these URLs are inquired frequently:

gs.bjtu.edu.cn, cn.linkedin.com, beijing.zhaopin.com, careers.microsoft.com, www.amazon.jobs, map.sogou.com.

Based on above descriptions, one can conclude the following scenario: a student from Beijing Jiaotong University is looking for a job or an internship position. The recruiting website he or she preferred is "Linkedin" at China and "Zhilian" at Beijing. It seems that the opportunities in "Microsoft" and "Amazon" are quite attractive for him or her. The online map service provided by "Sogou" is chosen to find the workplace locations and the suitable paths.

To relieve the risks of user privacy leakage within the DNS lookup process, we aim to design a smart collaborative distribution scheme guided by MTD.

3. The smart collaborative distribution

The foundation will be introduced to illustrate the preparation work of dynamic port hopping. Then, relevant steps and explanations are provided from end host's and DNS server's point of view.

3.1. Original assignments of port number

Two patterns have been summarized to distribute the available port number.

The first one is "static mode". According to the regulations of Internet Assigned Numbers Authority (IANA), the ordinary DNS function should listen port 53 for accepting the TCP or UDP queries, which means that the end host can respectively establish two flows through TCP 53 and UDP 53. New application for new port number occupation could be submitted to IANA. Nevertheless, the complex process and long discussions are indispensable. The attackers are also able to learn the new port numbers when they are approved. These facts illustrate that the "static mode" is not a good candidate for the smart collaborative distribution.

The second one is "dynamic mode". The port number could also be allocated to multiple users for a short period by DNS server when the queries are received. These temporary port numbers will be recycled for reutilization. Based on the description in RFC 6335 [10], the ports could be divided into three classes: "the Private or Ephemeral Ports" (from 49152 to 65535, never assigned), "the Registered Ports" (from 1024 to 49151, assigned by IANA) and "the Well Known Ports" (from 0 to 1023, assigned by IANA). The last two kinds of ports (i.e. from 0 to 49151) could be further labeled as "Reserved", "Unassigned" and "Assigned". Consequently, the "dynamic mode" will be more suitable for the smart collaborative distribution.

3.2. The algorithm used in end host

Similar with the original initialization process, the end host should configure the default DNS server correctly and test the basic packet exchanges.

If the user would like to enable the dynamic port hopping, the end host needs to confirm the new port number was allocated or not. Then, the period of port validity must be verified. If the new port number is still available, i.e. all the previous answers are "Yes", the URL resolving request could be sent to the new port number of DNS. When the new port number is not allocated or it is out of date, the port distribution request should be generated and transmitted to the DNS server automatically. The capacity of supporting dynamic port hopping should be checked. If the DNS server also enable such feature, a suitable acknowledgement should be transmitted to the end host. Then, the user can send the URL resolving request to the new port number of DNS. Both unsupported settings and unopened port will lead DNS server to initiate or repeat the port distribution again. If "No" is finally returned in this step, the DNS lookup can only be sent to the default port number.

If the user refuses to enable the dynamic port hopping, the original port of DNS is always opened. The diagram of detailed algorithm is shown in Fig. 1.

3.3. The algorithm used in DNS server

Comparing with the main procedures at the end host side, operations of DNS server are more complex. For simplification, we only introduce the case that dynamic port hopping is always supported. The traditional port number 53 for TCP and UDP should be listened since the DNS service was launched. When a dynamic port hopping request is captured, the recent opened port should be examined. If the port number is still usable, a message with SUCCESS primitive will be sent to the end host. The relevant notifications for intrusion detection, firewall and other security equipment must be executed to ensure the following DNS lookup will not be blocked.

When there is no recent opened port or the target port is expired, the DNS server need to determine whether a new port number should be issued to the user. For the "Yes" branch, one or more port numbers from resource pool can be chosen according to the allocation policy. If there is no available port number (i.e. all permitted ports are fully occupied), some ports might be recycled based on allocation time, priority, and other relevant parameters. If a new port number has been allocated successfully, one message with SUCCESS primitive should be returned to the user and notifications for security equipment must be made just like the previous case. For the "No" branch, the N/A primitive will be returned to the user. The user may also receive N/A primitive when no port number can be recycled immediately.

The diagram of detailed algorithm is shown in Fig. 2. The related threads should be established based on requirements to handle the DNS lookup on new port numbers (not shown in Fig. 2).

Algorithm 1 Dynamic Port Hopping (Initiative Side)

```
[Initializations for IP addresses, network connections, etc.]
while the URLs are ready
  if tradition method is needed then
    hopping_enable = 0;
    port = default port number;
  else
    hopping_enable = 1;
    if new port is allocated and still valid then
      port = allocated port number;
    else
      port = NULL;
    end if
  end if
[Negotiation with the DNS server]
  if hopping_enable = 1 and port = NULL then
    for each round in the loop
      if the SUCCESS primitive is received then
        port = new port number;
      else
        port = default port number;
      end if
    end for
  end if
[Send the lookup packet to the DNS server]
  for request number i from 1 to k step 1
    set the des_port_i = port;
  end for
    fill the other fields and send the packet;
end while
```

Fig. 1. Operations from end host's point of view.

A fact should be mentioned and emphasized: our smart collaborative distribution scheme is compatible with DNS Security Extensions (DNSSEC) [13,14]. The suggestions and recommendations during updating are introduced in [2,45].

3.4. The implementation scheme

To validate the practical performance, we implement the smart collaborative distribution into our prototype. A lot of open source software (such as BIND, PowerDNS, Unbound) is quite helpful during the DNS server establishment. Unbound is selected as the primitive protocol stack for necessary modifications. The dynamic port hopping feature is enabled for all equipment inside system. The packet exchanging between the end host and DNS server is captured and aggregated by Wireshark.

For the first step, we create DNS lookup and response packets in ordinary scenario. Then, modifications are made by a daemon program to change the corresponding field (four tuples, protocol type, application data, etc.) inside a packet. For instance, the source IP address and port number fields are set to "88.88.88.88" and "8888", respectively. By using the similar method, the generated DNS lookup packets will follow the predesigned rules.

For the second step, the dynamic port hopping can be achieved by referencing the packet structure suggested by RFC6891 [11]. The Extension mechanisms for DNS (EDNS) was created to remove previous restrictions and inspire more innovations for DNS community. Both the users and DNS servers are able to append new functionalities by following specific regulations. For instance, two IP addresses, 192.168.30.5 and 192.168.30.2, are assigned to the end host and DNS server, respectively. The first object illustrates that a DNS initiator is sent to the default DNS port. The destination port number 53 is displayed with hexadecimal form "00 35". The main body inside this packet is to apply for a new port number. The second object is the reply from DNS server to the user. The "Malformed Packet" sign in Wireshark means that the new packet format cannot be distinguished and explained by current version. Nevertheless, the details of the packet will still be demonstrated completely. Such sign will disappear if a specific plug-in is developed and embedded. The third object is a DNS lookup packet sent to the new port number. The destination and source port numbers are filled with 54444 and 33342, respectively in our measurement. The fourth object shows that the corresponding reply is sent via the new allocated port number 54444. Importantly, the end host and DNS server are able to resolve all exchanged packets correctly. The "Protocol" column in the third and fourth objects shows "UDP" (not "DNS" in the first and second objects) because

Algorithm 2 Dynamic Port Hopping (Passive Side)

```
[Initializations for firewall, listening daemon, etc.]
while the DNS service is enabled
  if a lookup packet is received then
    if a dynamic port hopping is required then
      port_searching = 1;
    else
      port_searching = 0;
    end if
  end if
[Searching for available port number]
  if port_searching = 1 then
    for possible port number i from 1 to k step 1
      if the capacity of i is sufficient then
        new_port = i;
      else if port number i can be successfully recycled then
        notify the corresponding end host;
        new_port = i;
      else
        new_port = NULL;
    end for
    if new_port != NULL then
      new_port_found = 1;
    end if
  end if
[Acknowledgement for the end host]
  if new_port_found = 1 then
    notify security equipments;
    send SUCCESS primitive back to the end host;
  else
    send N/A primitive back to the end host;
  end if
end while
```

Fig. 2. Operations from DNS server's point of view.

Wireshark may estimate the protocol type according to the destination and source port numbers. Both 54444 and 33342 are randomly selected and not classified as DNS-related ports. Therefore, these packets are only marked as "UDP".

4. Mathematical model and analysis

Although the details (assignments, algorithms, implementation, etc.) of the smart collaborative distribution have been provided, several interesting questions (optimal timing for ports retrieve, appropriate duration for ports occupation, logical size for ports pool, etc.) are still unanswered. Therefore, the analytical model should be proposed to explore the better performance of the system.

4.1. Modeling the dynamic port hopping

We select i to represent the single end host. Supposing the arriving rate r_{ai} of individual requests conforms to Poisson distribution, the entire arriving rate of requests

$$r_a = \sum_{i \in U} r_{ai}, \tag{1}$$

also follows Poisson distribution according to the superposition theorem. The end host set is represented by U. Supposing the service rate is r_s and the service period conforms to negative exponential distribution, if the service time of the nth request is t_n, then

$$P(t_n \le t) = 1 - e^{-r_s t}, \quad t \ge 0. \tag{2}$$

The probability density function of t_n should be

$$p(t_n) = r_s e^{-r_s t_n}, \quad t_n \ge 0. \tag{3}$$

The mathematical expectation of t_n can be expressed by

$$\begin{aligned} E(t_n) &= \int_{-\infty}^{+\infty} t_n p(t_n) \mathrm{d}t_n = \int_0^{+\infty} t_n r_s e^{-r_s t_n} \mathrm{d}t_n \\ &= r_s \cdot \left(-\frac{1}{r_s}\right) \int_0^{+\infty} t_n \mathrm{d}\left(e^{-r_s t_n}\right) \mathrm{d}t_n \\ &= -t_n e^{-r_s t_n}\Big|_0^{+\infty} + \int_0^{+\infty} e^{-r_s t_n} \mathrm{d}t_n \\ &= -\frac{1}{r_s} e^{-r_s t_n}\Big|_0^{+\infty} = \frac{1}{r_s}. \end{aligned} \tag{4}$$

If the size of port number pool, the usable ratio and the multiplex ratio are respectively represented by N_a, k and α, the equivalent port number m can be calculated by

$$m = \alpha \cdot k \cdot N_a. \tag{5}$$

For example, when the value of N_a is equal to 16384, if millesimal ports are allowed to be used triple times, there will be 49 qualified ports for the users.

When the DNS adopts “none buffer” scheme, the dynamic port hopping packets might be dropped if no available port number can be found. Motivated by Markov chain, the request number could be considered as the system state. The steady state probabilities p_n can be described in

$$r_a p_{n-1} = n r_s p_n, \quad n = 1,\ 2,\quad \ldots,\ m. \tag{6}$$

The expression of p_n will be

$$p_n = p_0 \left(\frac{r_a}{r_s}\right)^n \frac{1}{n!}, \quad n = 1,\ 2,\quad \ldots,\ m. \tag{7}$$

Since the summation of p_n includes all possibilities in system, it should be equal to 1, i.e.

$$\sum_{n=0}^{m} p_n = 1. \tag{8}$$

We can combine Eqs. (7) and (8) to achieve

$$\sum_{n=0}^{m} p_0 \left(\frac{r_a}{r_s}\right)^n \frac{1}{n!} = p_0 \sum_{n=0}^{m} \left(\frac{r_a}{r_s}\right)^n \frac{1}{n!}. \tag{9}$$

The probability of steady state 0 p_0 is an independent parameter. Therefore, it can be moved out of the summation notation. Then, we have

$$p_0 = \left[\sum_{n=0}^{m} \left(\frac{r_a}{r_s}\right)^n \frac{1}{n!}\right]^{-1}. \tag{10}$$

The blocking probability (i.e. m ports are fully utilized) is

$$p_m = \left(\frac{r_a}{r_s}\right)^m \frac{1}{m!} \Big/ \sum_{n=0}^{m} \left(\frac{r_a}{r_s}\right)^n \frac{1}{n!} \tag{11}$$

and the effective utilization could be calculated by

$$\beta_e = \left[1 - \left(\frac{r_a}{r_s}\right)^m \frac{1}{m!} \Big/ \sum_{n=0}^{m} \left(\frac{r_a}{r_s}\right)^n \frac{1}{n!}\right] \cdot \frac{r_a}{m r_s}. \tag{12}$$

Eq. (11) illustrates that the value of p_m is only related with r_a, r_s and m. If the end host aims to better control the blocking probability, then decreasing the request arriving rate, compressing the local process latency and increasing the equivalent port number would be the good options.

Eq. (12) indicates the occupation index of each equivalent port number. Due to multiplexing is allowed and suggested, different users can simultaneously access the same TCP or UDP port number inside DNS server. Therefore, the effective utilization of each port might be extremely high.

4.2. Performance analysis

The previous model presented theoretical relationships among multiple parameters. To further visualize the performance of the smart collaborative distribution, three scenarios are established from different perspectives: Firstly, the ratio values of

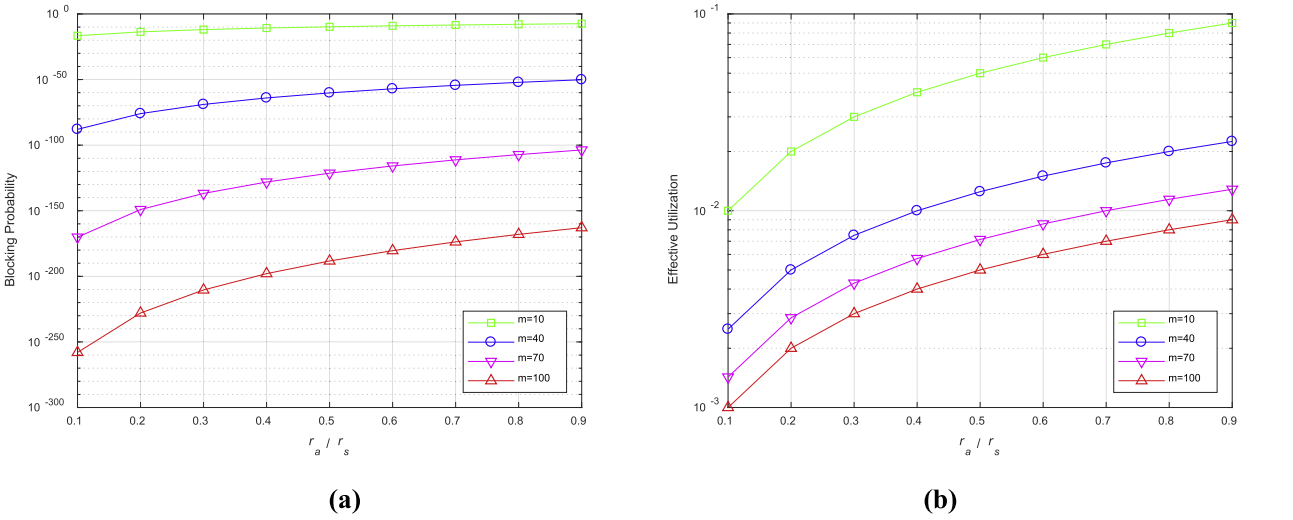

Fig. 3. Blocking probability and effective utilization when the ratio is smaller than one. (For interpretation of the references to color in this figure legend, the reader is referred to the web version of this article.)

arriving rate and service rate are limited within (0, 1). The fluctuations of blocking probability and effective utilization will be demonstrated in the logarithmic coordinate. Secondly, the values of such ratio are extended beyond 1. Similar targets in vertical axis will be focused and illustrated. Thirdly, the representative numbers of ports are provided. The results of privacy enhancement will be analyzed based on request ratio and distribution standard deviation.

Scenario 1: The request arriving rate is smaller than the service rate

The value of r_a/r_s is varying between 0.1 and 0.9 in Fig. 3(a). The blocking probability will be calculated based on identical increment (i.e. 0.1 for each step). If the value of equivalent port number is 100, the curve (marked with red line and up triangle) demonstrates nonlinear features distinctly. The minimum of p_m is 9.70E−259 when the value of r_a/r_s is equal to 0.1. When the value of m is decreased to 70, the blocking probability (marked with purple line and down triangle) will be further enhanced. The values in Y axis are 7.55E−171, 4.29E−122 and 2.13E−104 if 0.1, 0.5 and 0.9 are given in X axis. If the value of equivalent port number is 40, all results (marked with blue line and circle) are higher than that of the previous cases. The linear characteristic gradually appears. The values in Y axis are 1.11E−88, 6.76E−61 and 7.37E−51 when 0.1, 0.5 and 0.9 are selected in X axis. When the value of m is shrunk to 10, the curve of p_m (marked with green line and square) can be roughly treated as a straight line. If the value of r_a/r_s is equal to 0.1, the blocking probability is 2.49E−17. The middle and last values are 1.63E−10 (ratio value 0.5) and 3.91E−08 (ratio value 0.9).

The varying pattern of r_a/r_s is maintained in Fig. 3(b). The curve at the bottom illustrates the condition that the value of m is 100. The values of β_e for all situations are quite small due to the adequate ports provisioning. The minimum of this case is 1.00E−03 based on the curve. If reducing the value of equivalent port number to 70, all points will become greater than before. By decreasing the value of r_a/r_s, the β_e will be suppressed as well. Several representative points are 1.43E−03, 7.14E−03 and 1.29E−02 if values in X axis are 0.1, 0.5 and 0.9. When we modify the value of m to 40, the occupation index for each port number can be enhanced. The gap value of effective utilization will be 2.00E−02 when the values of r_a/r_s are equal to 0.1 and 0.9. If compressing the value of equivalent port number to 10, the peak value can be obtained (9.00E−02 in Y axis when 0.9 in X axis). The gap value of β_e is 8.00E−02 if the values of r_a/r_s are equal to 0.1 and 0.9. Since the logarithmic coordinate is utilized in Y axis, the differences among these four cases are much larger than they shown in Fig. 3(b).

Scenario 2: The request arriving rate is larger than the service rate

The value of r_a/r_s is changing between 100 and 900 in Fig. 4(a). For each 100 increment, the value of function will be drawn and analyzed. From macroscopic perspective, all the curves are converging to 1 with different speed if the value of parameter in X axis is increasing. If the value of m is 10, the value of p_m is equal to 9.01E−01 if the ratio is set to 100. The variation of blocking probability curve is not obvious. When the value of m is set to 40, 70 and 100, the increasing trend is gradually highlighted. We use difference values to represent such situation. If the range of ratio changed from 100 to 200, the corresponding difference values in Y axis will be 1.95E−01, 3.33E−01 and 4.29E−01 in blue, purple and red curves. These three values are 6.60E−02, 1.15E−01 and 1.64E−01 if the range of ratio changed from 200 to 300. The gaps among them are getting smaller and the blocking probability is quickly increased. The values of p_m are 9.89E−01, 9.56E−01, 9.22E−01 and 8.89E−01 if the ratio value is set to 900. Such phenomenon illustrates: when m is 100, there is still 10% success probability even if r_a is much larger than r_s. The minimum of p_m in Fig. 4(a) is 7.57E−02 when X axis value is 100, which indicates the success probability could be 92%.

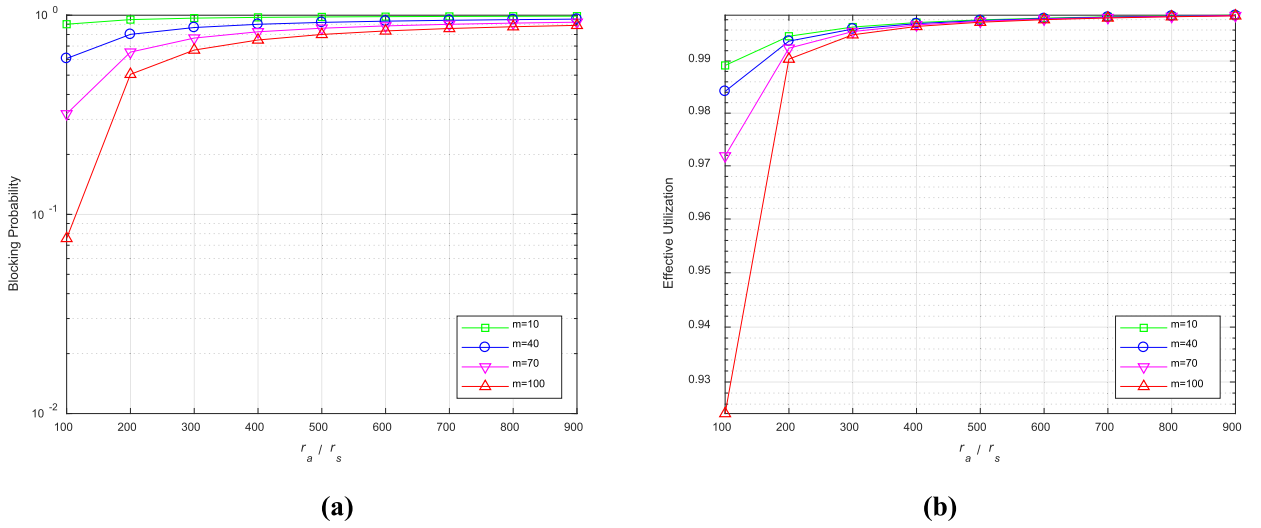

Fig. 4. Blocking probability and effective utilization when the ratio is larger than one. (For interpretation of the references to color in this figure legend, the reader is referred to the web version of this article.)

The changing pattern of r_a/r_s is maintained in Fig. 4(b). We notice the convergence rate is a bit higher than that of Fig. 4(a). And the final convergence values are also quite close with each other, i.e. 9.99E−01 for four curves, which means the equivalent ports are almost fully occupied. When the value in X axis is 100, the effective utilizations are 9.89E−01, 9.84E−01, 9.72E−01 and 9.24E−01 for green, blue, purple and red curves. Even the minimum in this case is still above 90%. Such characteristic remind us: if the request arriving rate is too high and the process period is too long, only abundant equivalent port number could relieve the average busy level. If the threshold value of utilization has been estimated, then one could employ Eq. (12) to calculate the minimum requirement of equivalent port number.

Scenario 3: Privacy enhancement analysis based on port number multiplex ratio

One important feature of our scheme is port selection. If the attacker successfully guessed the new port number assigned by DNS server, similar monitoring method could be launched. It is hard to eliminate the eavesdropping in current Internet. However, the difficulty of such action can be increased significantly. The port number of Traditional DNS (T-DNS) is fixed in existing network infrastructure. Our smart collaborative distribution scheme is not only compatible with it, but also friendly with other novel policies. We notice that the attackers may get all available ports by using “exhaustion inquiry” mechanism. In order to deploy effective defenses, the promising policy should reduce the possibility of being captured. When one end host applies for dynamic port hopping, the history will be checked and a fresh port number might be allocated. As the strong candidates, three policies are validated, i.e. Random Selection Distribution (RSD), Partial Range Distribution (PRD) and Full Range Distribution (FRD).

First, we analyze the request ratio value of four policies. The numerator is the request number of each port and the denominator is the overall request number. Such value shows the possible of privacy leakage when an attacker monitors a specific port. When setting the available port is 100 and request number is 100k, the distribution situation is illustrated in Fig. 5(a). For T-DNS case, all requests will be sent to the default port. Therefore, the request ratio for other ports is 0. For RSD case, the port is randomly selected, which leads to none uniform pattern. The maximum and minimum in Y axis are 0.06 and 0, respectively. For PRD case, the suitable scenario is when eavesdropping cost is very high for some specific ports. Then, our scheme can mainly distribute the requests to these ports on purpose. Another benefit in this case is the port number used for dynamic hopping could be reduced if a threshold is confirmed. In Fig. 5(a), 5% available ports are utilized for request distributions. It can meet the requirement if the threshold is less than or equal to 20%. For FRD case, the design target is to minimize the potential risk of port eavesdropping. For instance, no matter which port is under surveillance, only 1% DNS requests will be gathered, which is indeed a small portion for the whole system.

Second, more available ports are enabled in our scheme, which will further increase the difficulty of “exhaustion inquiry” attacks. The results are illustrated in Fig. 5(b). Since too many details are involved, several important points are not easily discovered, such as the request ratio for default port in T-DNS case. However, the distribution characteristic is not changed.

Third, the intermediate situations, i.e. the available port numbers between 200 and 900, are presented. To simplify the complex statistics, only standard deviation of distribution is demonstrated in Fig. 5(c). In T-DNS case, since only one port can be used, the value in Y axis is the highest comparing with other policies. In RSD case, the results are approaching to a line and the decline magnitude is not large. In PRD case, the requests are allocated to several specific ports, which also trigger the high standard deviation (between T-DNS and RSD curves). All these three cases are getting lower when the number of available ports is increasing. Since the FRD can uniformly utilize the ports, the standard deviation is always equal to 0.

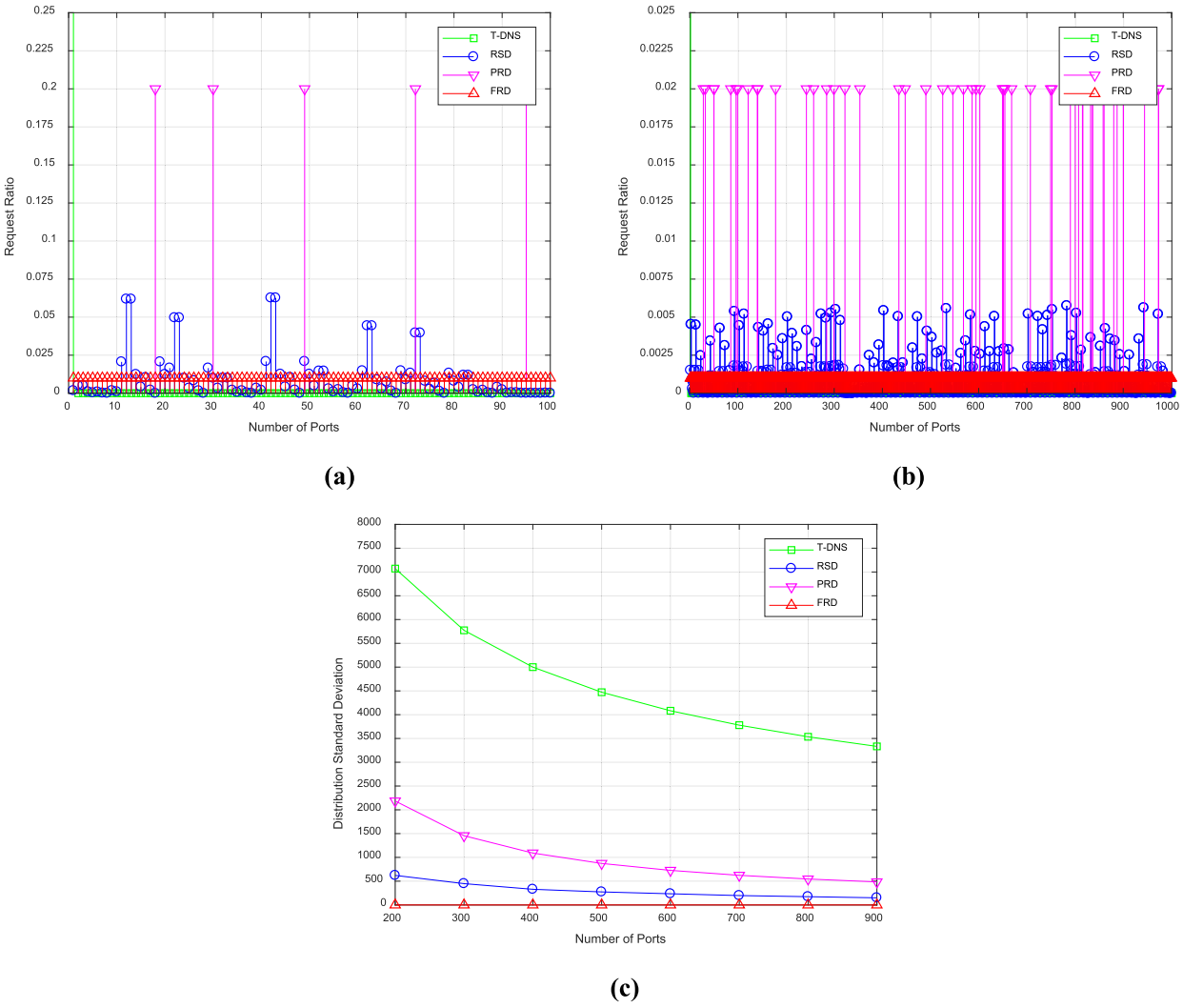

Fig. 5. Privacy enhancement analysis based on port number multiplex ratio.

5. Related work

In order to find the appropriate integration from privacy perspective, the latest progresses in MTD and DNS are carefully selected and compared. Based on the characteristics, each of them is separated into multiple categories during the discussions.

5.1. Methodology and applications of MTD

The conception of MTD has gained plenty of attentions from many communities since it was proposed. Carvalho and Ford [8] presented a high level overview of utilizing MTD in computer network. Building better resilience is an important viewpoint in this article. The authors also stated the challenges and promises of MTD in handling system complexity, fighting with intelligent adversaries, defining metrics, achieving coordination, etc. In the following, we classify the methodology and application literatures into four aspects.

Evaluation-based methods. Three evaluation mechanisms (metric, cost and assessment) are presented. Inspired by the biodiversity, Zhang et al. [49] proposed a novel model based on plenty of evaluations and analysis. Two complementary metrics in diversity were illustrated according to the average and the least efforts of attacking. The authors demonstrated the software diversity estimation as a case study and validated the novel schemes in simulation scenarios. Van Leeuwen et al. [40] deemed that the MTD will not only increase the complexity and uncertainty for the attackers, but also add more extra burdens for the original system. Therefore, the cost of network management can be boosted and the overall performance might be affected. To identify the specific impact of the MTD methods (in terms of the consumed computing and network

resources), this paper proposed a new term "defensive work factor". The MTD's influences of different services are analyzed and the deployment cost of the scheme is also provided. Following the similar idea, Van Leeuwen et al. [41] worried the outages of network may finally lead to inadequate capacity for attack defense. It would be useful if a practical MTD evaluation approach exists. By utilizing the defensive work factor, the authors presented the Application Performance Monitoring (APM) which executes assessment from user's point of view. Multiple attacking scenarios are involved for performance validations. However, these work mainly focused on evaluations. The privacy issues were not properly mentioned.

Parameter-based methods. Three parameters (IP address, port and path) are introduced. Yan et al. [46] focused on the frequency of IP address mutation which is a significant element for hijacking or sniffing defense in MTD. A scheme named Sliding WIndow and Full Transparent (SWIFT) was presented to handle the mutation of IPv6 address. The compatibility has been fully considered to guarantee the deployment in current network. The experiment results of prototype illustrated that SWIFT is efficient in different environments. More representative approaches of IP address mutation can be found in [43,23]. Based on MTD strategies, Thompson et al. [39] proposed a proactive scheme to suppress the ability of web server weakness probing. An implementation was accomplished and relevant details are also provided. The comprehensive validations showed that the diversity of web server is able to alleviate the influence of existing vulnerabilities and enhance the resilience of services. Although this paper attempted to redirect the original port, the mechanism could be smarter to deal with more complicated scenarios. Zhang et al. [48] adopted the Software Defined Network (SDN) to design path hopping approach. Satisfiability modulo theory was utilized to find the suitable paths. The candidates should meet the constraints of capacity and overlap. The collaboration details between the controller and switch were provided and analyzed. The evaluations showed that the latency of path hopping is acceptable. Although above parameters have been utilized in MTD, these works can be further improved for the privacy protection purpose, especially when dynamical scenarios are involved.

DDoS-oriented usages. Three Distributed Denial of Service (DDoS) scenarios (aggregation-based, proxy-based, and Crossfire-based) are compared. Jia et al. [25] introduced a new scheme named MOTAG to defend the flooding type DDoS. A cluster of secret proxies is aggregated to bypass the attack packets dynamically and protect legitimate users and selected servers. Since MOTAG may compel the attackers to collude with compromised insiders, a novel method was enabled to isolate the malicious insiders by changing the proxies. The designed algorithm is helpful in optimizing the proxy relocation and attack identification. By pointing out the shortages of MOTAG, Venkatesan et al. [42]described and implemented the "proxy harvesting attack". Since this new attack pattern is able to gather sufficient details about proxies before starting the DDoS, traditional approaches are not effective during the defense process. Then, the authors proposed a skillful MTD scheme by proactively and periodically changing the mapping relation between the user and the proxy. The theoretical and experimental validations illustrated the overall performance, in terms of proxy discovery and user isolation. Aydeger et al. [3] claimed the benefits of employing SDN and MTD in relieving the influence of DDoS. The Crossfire, one type of attack patterns, was chosen as the target during the investigation. Based on the property analysis, a novel scheme was proposed to avoid the link congestion when packets are forwarded. Nevertheless, whether the mutation of routes can limit the effects of DDoS and maintain the quality of services should be evaluated in depth.

Cloud-oriented usages. Three characteristics (game-theoretic, bandit and lightweight) are discussed in cloud environment. Adili et al. [1] firstly summarized the significance of cloud security and discussed the advantages of using MTD. Then, a defense scheme was proposed by focusing on Virtual Machines (VMs) migrations. The authors modeled the problem as a signaling game and found the Nash equilibria, which guarantees the efficiency of the approach. Penner and Guirguis [36] presented several MTD strategies by randomizing the VMs to defend Multi-Armed Bandit (MAB) attacks. The typical behavior of MAB that scan the locations of VMs and compare their rewards can be inhibited. Both the simulation and implementation results illustrated that the MTD strategies can limit the damage of MAB attacks. Azab and Eltoweissy [4] focused on the side-channel attacks that may obtain the information from the neighbor users. The authors insisted that the current solutions are not pervasive enough for different attack patterns, which bring unnecessary adjustments forbrk both the hardware and software. Therefore, a new scheme named MIGRATE was proposed to confuse the attackers and protect the target. However, the implementation results of MIGRATE could be analyzed via multiple perspectives.

5.2. Privacy enhancement of DNS

Due to the critical function of DNS, the hackers prefer to spend more efforts on developing modern attacking weapons. Since many privacy issues are inherent in DNS infrastructure, researchers have been looking for appropriate solutions for years. Here, we simply separate these work into two categories based on their peculiar properties.

Direct enhancement approaches. The privacy leakage during the DNS lookup process has been investigated based on different policies. Mohaisen et al. [34] analyzed the DNSSEC Look-aside Validation (DLV) to find the shortage of current version. Both the privacy implications and lax specifications are emphasized, which confirmed the privacy disclosure problem. By exploring the root reasons, the authors proposed two methods for privacy improvement. The costs of deployment and utilization are also provided. Yuchi et al. [47] verified the importance of DNS functionality by focusing on the privacy challenges. Possible leakage approaches together with the risks are presented and discussed. The authors exploited several criterions and proposed a preserving scheme for DNS privacy. The latency of DNS lookup is selected as the main parameter during the performance comparison. Di Bella et al. [12] identified that users' URL requests could seriously expose the sensitive information if unreliable entities are involved. A deployable scheme is proposed based on overlay pattern to enable the anonymous queries for DNS. The secret sharing method is utilized and each peer can operate as a proxy during the

implementation. The evaluations showed that the leakage probability could be reduced with the increasing of the hop number. By focusing on the DNS service discovery in multicast, Kaiser and Waldvogel [26] wanted to resolve the contradiction between "zero configuration" and information publicity. An enhanced approach is proposed to hide the useful information as much as possible. After the necessary initialization, almost no further configurations are required during the utilization. An open source software Avahi is adopted to illustrate the feasibility and the convenience of system upgrade is also highlighted. More performance analysis and comparison about this work can be found in [27]. After elaborately listing several risks in DNS, Zhu et al. [50] proposed a connection-oriented method T-DNS to solve them comprehensively. TCP and Transport-Layer Security (TLS) are employed to substitute UDP's functionality during the DNS lookup. Although such replacement may introduce more delays and system states, the paper proved that T-DNS could achieve more benefits with modest and limited cost. The authors also provided sufficient figures and tables to illustrate the overall performance. Kang and Mohaisen [28] investigated the privacy issue in special domain name environment and emphasized the significance of recommendations in practice. Different scenarios are established to assess the privacy protection capacity. Unfortunately, the details of comprehensive analysis were not fully provided due to the page or other reasons, which limited the application scope.

Indirect enhancement approaches. If massive domain information can be correctly collected by a specific entity, it is reasonable to outsource the tasks of malicious domain detection. Ma et al. [33] presented a system named DNSRadar to explore the current outsourcing service. By employing the link analysis approach, DNSRadar is able to estimate the multiple malicious domains. According to the information gathered from DNS servers, the authors illustrated large scale evaluations. Roughly 90% malicious domains can be detected with a false positive rate of 1%. Hesselman et al. [21] leveraged the control plane to improve the management of Top-Level Domains (TLDs). Original services of TLDs operator can be extended and the possible risks can be detected. Two key data sources, i.e. DNS traffic and registered domains, are adopted to achieve the main functionalities. The TLDs users' privacy can also be protected based on the experiments in Netherlands. After the comprehensive analysis of vulnerabilities and potential influences of DNS, Jalalzai et al. [24] designed a digital signature method for DNS based on DNSSEC and Berkeley Internet Name Domain (BIND) software. The implementation results showed the target function is accomplished. As one of the most famous anonymity network, Tor has created many novel services in a hidden way. Although domain ".onion" is supposed to be resolved inside Tor network, one could still see many related requests in public DNS. Mohaisen and Ren [35] attempted to capture the feature and pattern of such leakage based on two large DNS datasets. Many interesting findings (fluctuation of volume, correlation with geopolitical events, etc.) are discovered. To monitor the healthy condition of overall DNS, especially for the TLDs, Korczynski et al. [30] focused on two metrics of abuse (occurrence and persistence) and evaluated their performance based on three typical data traces. The authors pointed that the abuse of good reputation services may affect the whole TLDs. A regression model is also proposed based on statistical perspective for analysis. Wang and Xiao [44] concentrated their attention on a critical problem: How to renew the trust chain when the key is compromised? Such situation is reconstructed to find a suitable solution. The authors proposed a rollover scheme and discussed its performance via four perspectives. The latency of transition is also evaluated based on signed TLDs. Borgwart et al. [5] deemed that the hijacking attacks of domain name are harmful for services, users and networks. Therefore, the authors established a LookUp DIstributed Cache (LUDIC) system to avoid potential damages. Instead of centralization pattern, LUDIC utilized distributed approaches for DNS record validations. The compatibility with existing security equipment is fully considered as well. These papers are excellent in terms of proposal design and implementations. Nevertheless, the relationships between port utilization and privacy leakage are hardly mentioned.

6. Conclusions

Motivated by MTD applications in many related areas, we proposed a smart collaborative distribution scheme for privacy enhancement. Specifically, the DNS scenarios are focused due to the following reasons. Massive DNS lookup requests were sent by various electronic equipment inside the Internet. Such situation not only triggered enormous pressures for the DNS infrastructure, but also seriously led to privacy challenges. Therefore, the target of our solution is to achieve dynamic port hopping by leveraging the advantages of MTD. First, the preliminary and potential risks of DNS were introduced based on six types of DNS attack approaches, three different locations of DNS servers and four ways of DNS privacy leakages. Second, the details of the smart collaborative distribution were presented through two kinds of port number assignment schemes, specific procedures, implementation results, etc. Third, a mathematical model was established to analyze the performance quantitatively. Multiple parameters (such as diverse DNS rates, equivalent port number) are fully considered in different conditions. The results of blocking probability and effective utilization have illustrated that our smart collaborative distribution scheme can enhance the user privacy in complex environments.

Acknowledgments

We would like to thank all the reviewers and editors for their invaluable comments and efforts on this article. This work was supported by the Fundamental Research Funds for the Central Universities under grant no. 2017JBM012 and The Soonchunhyang University Research Fund.

References

[1] M.T. Adili, A. Mohammadi, M.H. Manshaei, M.A. Rahman, A cost-effective security management for clouds: a game-theoretic deception mechanism, in: 2017 IFIP/IEEE Symposium on Integrated Network and Service Management (IM), Lisbon, Portugal, 2017, pp. 98–106.
[2] R. Arends, R. Austein, M. Larson, D. Massey, and S. Rose, Protocol Modifications for the DNS Security Extensions. RFC 4035, 2005.
[3] A. Aydeger, N. Saputro, K. Akkaya, M. Rahman, Mitigating crossfire attacks using SDN-based moving target defense, in: 2016 IEEE 41st Conference on Local Computer Networks (LCN), Dubai, 2016, pp. 627–630.
[4] M. Azab, M. Eltoweissy, MIGRATE: towards a lightweight moving-target defense against cloud side-channels, in: 2016 IEEE Security and Privacy Workshops (SPW), San Jose, CA, 2016, pp. 96–103.
[5] A. Borgwart, S. Boukoros, H. Shulman, C. van Rooyen, M. Waidner, Detection and forensics of domains hijacking, in: 2015 IEEE Global Communications Conference (GLOBECOM), San Diego, CA, 2015, pp. 1–6.
[6] M. Calder, X. Fan, Z. Hu, E. Katz-Bassett, J. Heidemann, R. Govindan, Mapping the expansion of Google's serving infrastructure, in: Proceedings of the 2013 Conference on Internet Measurement Conference (IMC '13), New York, NY, USA, ACM, 2013, pp. 313–326.
[7] T. Callahan, M. Allman, M. Rabinovich, On modern DNS behavior and properties, SIGCOMM Comput. Commun. Rev. 43 (July (3)) (2013) 7–15.
[8] M. Carvalho, R. Ford, Moving-Target Defenses for Computer Networks, IEEE Secur. Privacy 12 (March–April (2)) (2014) 73–76.
[9] R. Chitpranee, K. Fukuda, Towards passive DNS software fingerprinting, in: Proceedings of the 9th Asian Internet Engineering Conference (AINTEC '13), New York, NY, USA, ACM, 2013, pp. 9–16.
[10] M. Cotton, L. Eggert, J. Touch, M. Westerlund, and S. Cheshire, Internet Assigned Numbers Authority (IANA) Procedures for the Management of the Service Name and Transport Protocol Port Number Registry. RFC 6335, 2011.
[11] J. Damas, M. Graff, and P. Vixie, Extension Mechanisms for DNS (EDNS(0)). RFC 6891, 2013.
[12] G. Di Bella, C. Barcellona, I. Tinnirello, A secret sharing scheme for anonymous DNS queries, in: AEIT Annual Conference 2013, Mondello, 2013, pp. 1–5.
[13] D. Eastlake, Domain Name System Security Extensions. RFC 2535, 1999.
[14] D. Eastlake and C. Kaufman, Domain Name System Security Extensions. RFC 2065, 1997.
[15] A. Ekert, R. Renner, The ultimate physical limits of privacy, Nature 507 (7493) (2014) 443–447.
[16] A.D. Ferguson, J. Place, R. Fonseca, Growth analysis of a large ISP, in: Proceedings of the 2013 Conference on Internet Measurement Conference (IMC '13), New York, NY, USA, ACM, 2013, pp. 347–352.
[17] H. Gao, V. Yegneswaran, Y. Chen, P. Porras, S. Ghosh, J. Jiang, H. Duan, An empirical reexamination of global DNS behavior, in: Proceedings of the ACM SIGCOMM 2013 Conference on SIGCOMM (SIGCOMM '13), New York, NY, USA, ACM, 2013, pp. 267–278.
[18] N.M. Hands, B. Yang, R.A. Hansen, A study on botnets utilizing DNS, in: Proceedings of the 4th Annual ACM Conference on Research in Information Technology (RIIT '15), New York, NY, USA, ACM, 2015, pp. 23–28.
[19] S. Hao, M. Thomas, V. Paxson, N. Feamster, C. Kreibich, C. Grier, S. Hollenbeck, Understanding the domain registration behavior of spammers, in: Proceedings of the 2013 Conference on Internet Measurement Conference (IMC '13), New York, NY, USA, ACM, 2013, pp. 63–76.
[20] A. Herzberg, H. Shulman, DNS authentication as a service: preventing amplification attacks, in: Proceedings of the 30th Annual Computer Security Applications Conference (ACSAC '14), New York, NY, USA, ACM, 2014, pp. 356–365.
[21] C. Hesselman, G.C.M. Moura, R.d.O. Schmidt, C. Toet, Increasing DNS security and stability through a control plane for top-level domain operators, IEEE Commun. Mag. 55 (January (1)) (2017) 197–203.
[22] V. Heydari, S.i. Kim, S.M. Yoo, Scalable anti-censorship framework using moving target defense for web servers, IEEE Trans. Inf. Forensics Secur. 12 (May (5)) (2017) 1113–1124.
[23] J.H. Jafarian, E. Al-Shaer, Q. Duan, An effective address mutation approach for disrupting reconnaissance attacks, IEEE Trans. Inf. Forensics Secur. 10 (December (12)) (2015) 2562–2577.
[24] M.H. Jalalzai, W.B. Shahid, M.M.W. Iqbal, DNS security challenges and best practices to deploy secure DNS with digital signatures, in: 2015 12th International Bhurban Conference on Applied Sciences and Technology (IBCAST), Islamabad, 2015, pp. 280–285.
[25] Q. Jia, K. Sun, A. Stavrou, MOTAG: moving target defense against internet denial of service attacks, in: 2013 22nd International Conference on Computer Communication and Networks (ICCCN), Nassau, 2013, pp. 1–9.
[26] D. Kaiser, M. Waldvogel, Adding privacy to multicast DNS service discovery, in: 2014 IEEE 13th International Conference on Trust, Security and Privacy in Computing and Communications, Beijing, 2014, pp. 809–816.
[27] D. Kaiser, M. Waldvogel, Efficient privacy preserving multicast DNS service discovery, in: 2014 IEEE Intl Conf on High Performance Computing and Communications, 2014 IEEE 6th Intl Symp on Cyberspace Safety and Security, 2014 IEEE 11th Intl Conf on Embedded Software and Syst (HPCC,CSS,ICESS), Paris, 2014, pp. 1229–1236.
[28] A.R. Kang, A. Mohaisen, Assessing DNS privacy under partial deployment of special-use domain names, in: 2016 IEEE Conference on Communications and Network Security (CNS), Philadelphia, PA, 2016, pp. 358–359.
[29] I. Khalil, T. Yu, B. Guan, Discovering malicious domains through passive DNS data graph analysis, in: Proceedings of the 11th ACM on Asia Conference on Computer and Communications Security (ASIA CCS '16), New York, NY, USA, ACM, 2016, pp. 663–674.
[30] M. Korczynski, S. Tajalizadehkhoob, A. Noroozian, M. Wullink, C. Hesselman, M.v. Eeten, Reputation metrics design to improve intermediary incentives for security of TLDs, in: 2017 IEEE European Symposium on Security and Privacy (EuroS&P), Paris, 2017, pp. 579–594.
[31] S. Landau, Control use of data to protect privacy, Science 347 (6221) (2015) 504–506.
[32] C. Lei, D.H. Ma, H.Q. Zhang, Optimal strategy selection for moving target defense based on Markov game, IEEE Access 5 (2017) 156–169.
[33] X. Ma, J. Zhang, J. Tao, J. Li, J. Tian, X. Guan, DNSRadar: outsourcing malicious domain detection based on distributed cache-footprints, IEEE Trans. Inf. Forensics Secur. 9 (November (11)) (2014) 1906–1921.
[34] A. Mohaisen, Z. Gu, K. Ren, Privacy implications of DNSSEC look-aside validation, in: 2017 IEEE 37th International Conference on Distributed Computing Systems (ICDCS), Atlanta, GA, USA, 2017, pp. 2438–2443.
[35] A. Mohaisen and K. Ren, "Leakage of .onion at the DNS root: measurements, causes, and countermeasures," in IEEE/ACM Transactions on Networking IEEE/ACM Trans. Networking, vol.PP, no. 99, pp.1–14.
[36] T. Penner, M. Guirguis, Combating the bandits in the cloud: a moving target defense approach, in: 2017 17th IEEE/ACM International Symposium on Cluster, Cloud and Grid Computing (CCGRID), Madrid, Spain, 2017, pp. 411–420.
[37] H. Shulman and S. Ezra, POSTER: on the resilience of DNS infrastructure. In Proceedings of the 2014 ACM SIGSAC Conference on Computer and Communications Security(CCS '14). ACM, Ne w York, NY, USA, 1499–1501.
[38] F. Song, W. Quan, T. Zhao, H. Zhang, Z. Hu, I. You, Ports distribution management for privacy protection inside local domain name system, in: ACM CCS MIST, 2016, pp. 81–87.
[39] M. Thompson, M. Mendolla, M. Muggler, M. Ike, Dynamic application rotation environment for moving target defense, in: 2016 Resilience Week (RWS), Chicago, IL, 2016, pp. 17–26.
[40] B.P. Van Leeuwen, W.M.S. Stout, V.E. Urias, Operational cost of deploying moving target defenses defensive work factors, in: MILCOM 2015 - 2015 IEEE Military Communications Conference, Tampa, FL, 2015, pp. 966–971.
[41] B.P. Van Leeuwen, W.M.S. Stout, V.E. Urias, Empirical assessment of network-based moving target defense approaches, in: MILCOM 2016 - 2016 IEEE Military Communications Conference, Baltimore, MD, 2016, pp. 764–769.
[42] S. Venkatesan, M. Albanese, K. Amin, S. Jajodia, M. Wright, A moving target defense approach to mitigate DDoS attacks against proxy-based architectures, in: 2016 IEEE Conference on Communications and Network Security (CNS), Philadelphia, PA, 2016, pp. 198–206.
[43] S. Wang, L. Zhang, C. Tang, A new dynamic address solution for moving target defense, in: 2016 IEEE Information Technology, Networking, Electronic and Automation Control Conference, 2016, pp. 1149–1152.

[44] Z. Wang, L. Xiao, Emergency key rollover in DNSSEC, in: 2014 IEEE 13th International Conference on Trust, Security and Privacy in Computing and Communications, Beijing, 2014, pp. 598–604.
[45] S. Weiler and D. Blacka, Clarifications and Implementation Notes for DNS Security (DNSSEC). RFC 6840, 2013.
[46] S. Yan, X. Huang, M. Ma, P. Zhang, Y. Ma, A novel efficient address mutation scheme for IPv6 networks, IEEE Access 5 (2017) 7724–7736.
[47] X. Yuchi, G. Geng, Z. Yan, X. Lee, Towards tackling privacy disclosure issues in domain name service, in: 2017 IFIP/IEEE Symposium on Integrated Network and Service Management (IM), Lisbon, Portugal, 2017, pp. 813–816.
[48] L. Zhang, Q. Wei, K. Gu, H. Yuwen, Path hopping based SDN network defense technology, in: 2016 12th International Conference on Natural Computation, Fuzzy Systems and Knowledge Discovery (ICNC-FSKD), 2016, pp. 2058–2063.
[49] M. Zhang, L. Wang, S. Jajodia, A. Singhal, M. Albanese, Network diversity: a security metric for evaluating the resilience of networks against zero-day attacks, IEEE Trans. Inf. Forensics Secur. 11 (May (5)) (2016) 1071–1086.
[50] L. Zhu, Z. Hu, J. Heidemann, D. Wessels, A. Mankin, N. Somaiya, Connection-oriented DNS to improve privacy and security, in: 2015 IEEE Symposium on Security and Privacy, San Jose, CA, 2015, pp. 171–186.