POSTER:Quantitative Security Assessment Method based on Entropy for Moving Target Defense

Duohe Ma
State Key Laboratory Of Information Security
Institute of Information Engineering,CAS
Beijing, China
maduohe@iie.ac.cn

Liming Wang*
State Key Laboratory Of Information Security
Institute of Information Engineering,CAS
Beijing, China
wangliming@iie.ac.cn

Cheng Lei
China National Digital Switching System Engineering & Technological Research Center
Zhengzhou Henan China
leicheng12150@126.com

Zhen Xu
State Key Laboratory Of Information Security
Institute of Information Engineering,CAS
Beijing, China
xuzhen@iie.ac.cn

Hongqi Zhang
China National Digital Switching System Engineering & Technological Research Center
Zhengzhou Henan China
zhq37922@126.com

Meng Li
Department of Computer Science
Hong Kong Baptist University
Hong Kong SAR, China
mli@comp.hkbu.edu.hk

ABSTRACT

Moving Target Defense(MTD) provides a promising solution to reduce the chance of weakness exposure by constantly changing the target's attack surface. Though lots of MTD technologies have been researched to defend network attacks, there is little systematic study on security assessment of MTD. This paper proposes a novel method to quantify the security of MTD system which based on three factors: Vulnerability Entropy, Attack Entropy and Attenuation Entropy. This assessment model provides a theoretical and practical guidance for building MTD system and improving MTD technology.

CCS Concepts

•**Security and privacy → Network security;**

Keywords

Moving Target Defense; Network Security; Quantitative Assessment; Entropy

1. INTRODUCTION

Moving Target Defense is a new promising defense technology which is able to automatically change one or more systematic attributes, rendering attack surface unpredictable for attackers. It effectively limits exposure of vulnerabilities that maybe exploited by attackers through diverse and dynamic changes in building of deployment mechanisms and strategies to increase the difficulty and cost of attacks[1].

Current studies mainly focus on design and implementation of new MTD technologies,such as Address Space Randomization (ASR)[2], Instruction Set Randomization (ISR)[3], and Data Randomization (DR)[4], while paying little attention on its security assessment[5]. Whereas, without qualitative or quantitative security assessment, it is impossible to know the improvement in system security by its application or its own deficiencies and weaknesses.

In this paper, we propose a new Quantitative Security Assessment Method based on Entropy(named QSAME), which takes into account comprehensively defense shifting space, defense shifting frequency and the attack shifting frequency. Our method measures vulnerabilities of target system and quantifies its security by calculating the changes of vulnerability entropy of target system under MTD model.

2. ENTROPY IN MOVING TARGET DEFENSE

2.1 Key Parameters to MTD Security

Mandhata et al.[6] proposed a concept of system attack surface and quantify attack surface of the system by calculating security values of the system in three dimensions of function, channel and data.According to the definition of system attack surface, reduction in the number of features of attack surfaces can enhance the security of system.

However, the security assessment method for MTD based on attack surface has many defects. For example, the shifting space for elements are not defined, the shift frequencies for each attribute are not specified and the attack's frequencies are not considered.

Analysis and abstraction above of MTD model shows that given the type and number of system attributes, their $shifting$

[*] The corresponding author.

ASIA CCS '17 April 02-06, 2017, Abu Dhabi, United Arab Emirates
© 2017 Copyright held by the owner/author(s).
ACM ISBN 978-1-4503-4944-4/17/04.
DOI: http://dx.doi.org/10.1145/3052973.3055161

space and shifting frequency are key parameters influencing MTD security under certain *attack frequency.*

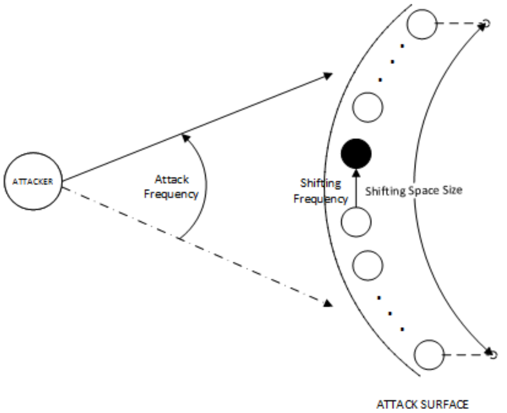


Figure 1: Key Parameters to MTD Security.

The shifting space of attributes is a set or range of replaceable values that the attributes may have in guarantee of system availability.

If one or more attributes change, the attack surface shifts. Therefore, individual shifting of the attributes and the overall shifting of attack surface are not completely synchronic.

2.2 Entropy in MTD Model

In information theory, entropy[18]is the counterpart of information, which means that greater entropy leads to greater uncertainty and less information.

Entropy is the most important metric of redundancy and diversity of MTD. We propose a new quantitative security assessment model to measure the security of MTD by analyzing the changes of information entropy during the shifting of attack surface. We hereby focus on security analysis of MTD model with a single attribute.

Table 1: The main notions used in this paper

Character	**Description**
$X = \{x_1, x_2, ..., x_N\}$	Attribute of MTD, where N is shifting space
$Y = \{y_1, y_2, ..., y_M\}$	Attack Vector,where M is attack times
$F^d = \{f_d(1), f_d(2), ..., f_d(N)\}$	Defense Shifting Frequency
$F^a = \{f_a(1), f_a(2), ..., f_a(M)\}$	Attack Frequency
β	Viscosity of Attack

The important assumption is that the attacker has to continuously attack x_i at least β times to confirm if it contains vulnerability. That is, $\beta \in \mathbb{N}^*$ represents the viscosity of attacks.

2.3 Security Assessment Based on Entropy

We use S_{mtd} to establish a security assessment model

$$S_{mtd} :< X, f_d, Y, f_a, \beta, T >$$

During the tim [0 T], it is related with X,f_d,Y,f_a and β. S_{mtd} can be calculated by Vulnerability Entropy,Attack Entropy and Attenuation Entropy. The definition and details will be given following.

Definition 1. (Vulnerability Entropy)The vulnerability entropy of X, denoted by $H_d(X)$, is defined as

$$H_d(X) = -\sum_{i=1}^{N} p(x_i) \log p(x_i). \quad (1)$$

Definition 2. (Attack Entropy) The attack entropy is defined as

$$H_a(Y|X) = -\sum_{j=1}^{M} p(y_j|X) \log p(y_j|X). \quad (2)$$

Definition 3. (Attenuation Entropy) We denote $H_w(X, f_d, t)$ as the value deducted from vulnerability entropy of X at time $t \in [0, T]$,

$$H_w(X, f_d, t) = \frac{[\frac{t \cdot f_d}{N}]}{[\frac{t \cdot f_d}{N}] + N} H_d(X). \quad (3)$$

Definition 4. (Security of MTD) The security of attribute X is co-determined by vulnerability entropy $H_d(X)$, attack entropy $H_a(Y|X)$ and attenuation entropy $H_w(X, f_d, t)$ during time $[0, T]$. The security of MTD at time $t \in [0, T]$, denoted by $S_{mtd}(X, t)$, is defined as

$$S_{mtd} = \lambda_d H_d(X) - \lambda_a H_a(Y|X) - \lambda_w H_w(X, f_d, t) \quad (4)$$

where $\lambda_d, \lambda_a, \lambda_w$ are weight parameters.

3. ANALYSIS AND APPLICATION

In an MTD system, the security S_{mtd} of attribute X is positively related to the entropy of vulnerability and decreases as attack entropy and attenuation entropy increase. In this paper, we consider S_{mtd} for the simplest case $\lambda_d = \lambda_w = 1$,$\lambda_a = \frac{\log N}{\log \beta}$. For $t < \frac{N}{f_d}$, $H_w(X, f_d, t) = 0$ and thus

$$S_{mtd} = H_d(X) - \frac{\log N}{\log \beta} H_a(Y|X)$$

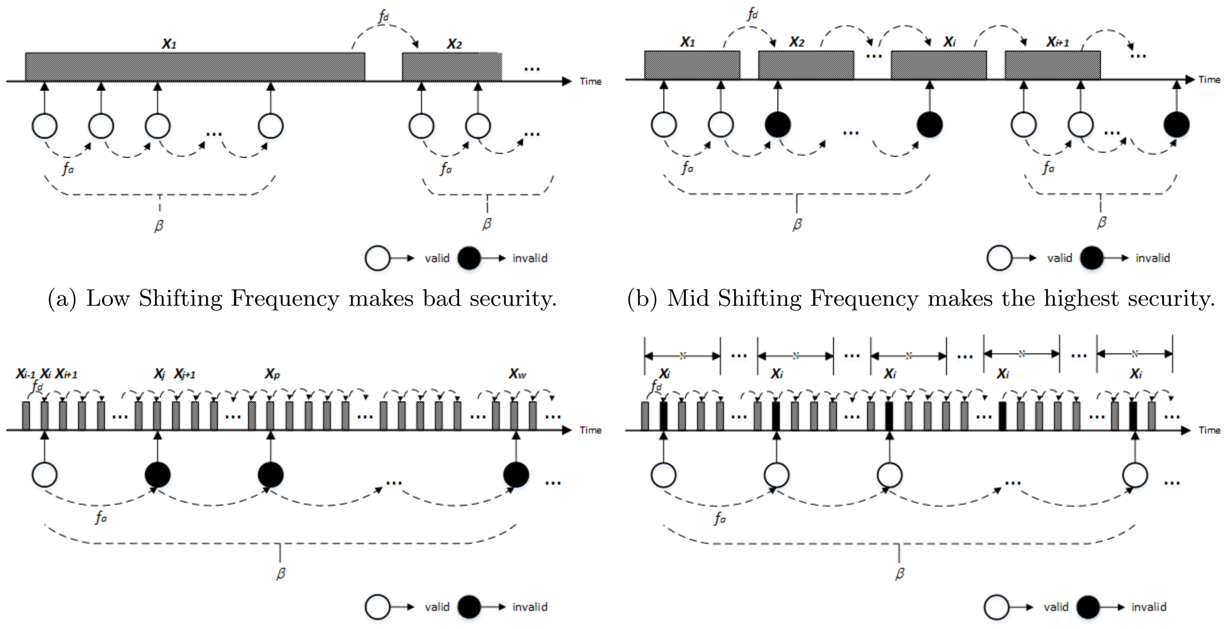
From further analysis of MTD modeląŕs quantitative security assessment method based on information entropy, we can obtain the following theorems assuming that $p(x_i) = 1/N$ for $x_i \in X$ and $p(y_j) \in \{0, \frac{1}{\beta}\}$ for $y_j \in Y$ (if the attack event y_j in β times continuously attacks which can confirmed a vulnerability then $p(y_j) = \frac{1}{\beta}$, otherwise $p(y_j) = 0$).

3.1 Shifting Space

Given the shifting space size N, the security of MTD $S_{mtd}(X)$ will be $\log N$. It means that if one MTD model has a bigger N, it will have a good start in security. Enlarging the shifting space N as great as possible is one effective way to increase security of MTD.

3.2 Shifting Frequency

At low shifting frequency as Fig.2(a) shows, for $f_d \leq f_a/\beta$, the attacker is able to confirm whether x_i is a vulnerability by β times of attacks in succession before X shifts during the time of a period $[0, \frac{1}{f_d})$. For $t \leq \frac{N}{f_d}$, $H_w(X, f_d, t) = 0$. Thus, when $t = \frac{\beta N}{f_a}$, we have $S_{mtd} = H_d(X) - \lambda_a H_a(Y|X) = \log N - \log N = 0$,which means system security is reduced to the minimum.



(a) Low Shifting Frequency makes bad security.

(b) Mid Shifting Frequency makes the highest security.

(c) When $f_d > f_a$ and $N \cdot f_a \nmid f_d$,attacks will fail.

(d) When $f_d > f_a$ and $N \cdot f_a | f_d$,attack will succeed.

Figure 2: Assessment Different Shifting Frequencies in MTD.

If $f_a/\beta < f_d \le f_a$, the attacker may finish some but not β times of attacks on x_i before attribute X shifts. Thus, the probability of detecting a vulnerability for the attack $p(y_j) = 0$. For $t \le \frac{N}{f_d}$ $H_w(X, f_d, t) = 0$, we can get $S_{mtd}(MAX) = H_d(X)$ -$\lambda_a H_a(Y|X)$= $H_d(X) - 0 = \log N$. The result shows in Fig.2(b) that when $f_a/\beta < f_d \le f_a$, shifting attribute will increase system security.

As show in Fig.2(c), when $f_d > f_a$ and $Nf_a \nmid f_d$, the attacker cannot attack the same x_i continuously, so $H_a(Y|X) = 0$ and $S_{mtd} = H_d(X) - H_w(X, f_d, t) = (\frac{N}{[\frac{t \cdot f_d}{N}]+N}) \log N$. It means that $S_{mtd}(X, t)$ will attenuate with $H_w(X, f_d, t)$ and can limit to 0 only when time t trends to $+\infty$.

Not all shiftiness will improve system security,even at high shifting frequency. When $N \cdot f_a | f_d$ as show in Fig.2(d), the attacker can attack the same x_i continuously in every $t_a = \frac{1}{f_a} = \theta * T_N$ cycles(θ=$\frac{f_d}{N \cdot f_a}$=1,2,...k) and confirm a vulnerability every $T_A = \beta \cdot t_a = \frac{\beta}{f_a}$ cycles. Thus, for the case $N \cdot f_a | f_d$ at time $t = N \cdot T_A = \frac{\beta N}{f_a} = \frac{\beta N^2 \theta}{f_d}$, we have $H_d(X) = \lambda_a H_a(Y|X) = \log N$, and $S_{mtd} = H_d(X) - \lambda_a H_a(Y|X) - H_w(X, f_d, t) \approx H_d(X) - \lambda_a H_a(Y|X) = 0$. This indicates that at this high shift frequency situaiton it is even worse to MTD model.

3.3 Security Attenuation

In given time $[0, T]$, as a part of the values of attribute X shifted by MTD are exposed after being used, its vulnerability entropy will continue to decrease. From the above definitions, we can see that$H_w(X, f_d, \infty) = H_d(X)$.

The higher value of H_w means more serious the exposure of attributes and poorer system security.

4. CONCLUSION

In this paper we first apply entropy theory into security analysis of MTD in network, which is more objective than other metrics. Our model measures system security by calculating the change of information entropy in system's attribute by shifting attack surface.

5. ACKNOWLEDGMENTS

This paper is supported by 973 Program of China (2011CB 311801); 863 Program of China (2012AA012704, 2015AA016106); the Strategic Priority Research Program of CAS (XDA06010701, XDA06010306); Zhengzhou Science and Technology Talents (131PLKRC644); "Young Scientist Program" of Institute of Information Engineering CAS (No.118800808).

6. REFERENCES

[1] S. Jajodia et al., Moving-Target Defense: Creating Asymmetric Uncertainty for Cyber Threats, Springer(2011)

[2] Shacham, Hovav, et al. On the effectiveness of address-space randomization. the 11th ACM conference on Computer and communications security.(2004).

[3] Gaurav S. Kc et al. Countering Code-Injection Attacks with Instruction-Set Randomization. In 10th ACM Conference on Computer and Communications Security (CCS)(2003)

[4] A. Nguyen-Tuong et al., Security through Redundant Data Diversity. Proc. IEEE Intąŕl Conf. Dependable Systems and Networks with FTCS and DCC(2008).

[5] Xu, Jun, et al. Comparing Different Moving Target Defense Techniques. Proceedings of the First ACM Workshop on Moving Target Defense. ACM(2014).

[6] Manadhata P K, Wing J M. A formal model for a systemąŕs attack surface[M]. Springer New York(2011)