DOI 10.15302/J-SSCAE-2016.06.015

Applying a Combination of Mimic Defense and Software Diversity in the Software Security Industry

Pang Jianmin[1], Zhang Yujia[1], Zhang Zheng[1], Wu Jiangxing[2]

1. State Key Laboratory of Mathematical Engineering and Advanced Computing, PLA Information Engineering University, Zhengzhou 450001, China
2. National Digital Switching System Engineering & Technological R&D Center, PLA Information Engineering University, Zhengzhou 450002, China

Abstract: With the development of the Internet, the process of computer software globalization continues to advance. A lot of identical software is installed on tens of thousands of computers. This makes widespread exploitation of software vulnerabilities easy and attractive for an attacker because the same attack vector will probably successfully affect numerous targets. Traditional software security methods can only be used to repair the vulnerabilities. Although software-diversity technology can remove the threat momentarily, it cannot eliminate the risk caused by vulnerabilities. This paper proposes a scheme of combining software diversity and mimic defense in the software security industry to eliminate the threat.
Keywords: software diversity; mimic defense; software security industry

1 Introduction

As early as the 10th Five-Year Plan, China had clearly proposed prioritizing the development of the information industry in economic and social fields to promote industrialization. The recent 13th Five-Year Plan also suggests that China should focus on the development of cybersecurity and informatization, safeguard the security of national network infrastructure, important information systems, and data resources, as well as should improve network management capabilities to assure the security of national information. China should also focus on the innovation of information management, information protection, security review, and other key technologies to meet the fundamental cybersecurity requirement of national development. As the foundation of cyberspace security industry, the software security industry is the driving force for promoting world economic growth and social development in the 21st century. The software security industry represents the national strategic direction and a wind vane of national economic development. It has become one of key competitiveness regarding national economic, social, and political security for a country. In the process of advancement of the international software security industry, developed and developing countries choose different paths and modes. It is necessary to start from the theory of economics to construct and choose a suitable software security industry development model. Thus, China must adopt a new mode to develop software security industry based on the current conditions of the software security industry of China, and that is, therefore, of tremendous significance.

Currently, mimic defense technology involves mimic computing and mimic defense technology systems that are based on multidimensional reconstructed functional architecture and dynamic multivariate operation mechanisms, and it is focused on achieving high efficiency and security of computing. Mimic defense technology is mainly directed against the notable asymmetry between the cyberspace attack and defense costs, and the seriousness of the information technology core and industrial base of China lagging behind national security demands. It is a type

Received date: 8 October 2016; **revised date:** 28 October 2016
Corresponding author: Pang Jianmin, State Key Laboratory of Mathematical Engineering and advanced computing, PLA Information Engineering University, Professor. Major research fileds include logic and information security. E-mail: jianmin_pang@hotmail.com
Funding program: CAE Major Advisory Project "Research on Cyberspace Security Strategy" (2015-ZD-10)
Chinese version: Strategic Study of CAE 2016, 18 (6): 074–078
Cited item: Pang Jianmin et al. Applying a Combination of Mimic Defense and Software Diversity in the Software Security Industry. *Strategic Study of CAE*, http://10.15302/J-SSCAE-2016.06.015

of revolutionary technology that modifies the rules of industry development and attempts to reverse the current cyberspace "easy to attack, difficult to defend" strategic pattern.

2 Security status of the software industry of China

2.1 Security problems in the software industry

2.1.1 Attack software vulnerabilities

On August 23, 2016, the China Internet Network Information Center (CNNIC) released the 38th Statistical Report on Internet Development in China, which revealed that up to June 2016, China's Internet users have reached 710 million, and the Internet penetration rate has reached 51.7%, indicating that half of the China's population has access to the Internet. However, this number is increasing constantly. As an important carrier of the development of the Internet, software has penetrated all areas of people's lives; thus, it has become the target of attackers. This suggests that users are increasingly being threatened by malicious software. In 2015, a team from the security company Secunia scanned 2 484 software programs obtained from 263 software vendors and discovered a total of 16 081 vulnerabilities; compared to 2014 and 2010, this was a total increase of 2% and 39%, respectively. The researchers determined that of all the successfully detected vulnerabilities, a majority (45.6%) were not important, 25.5% were medium-risk security vulnerabilities, 13.3% were high-risk security vulnerabilities, and 0.5% were extremely dangerous. In the vulnerability classification, 57% of the vulnerabilities were accessed through remote network access, 35% through the local network, and a small portion (8%) required the computer of the victim to trigger defects. ANSI/IEEE Std 729-1983: IEEE Standard Glossary of Software Engineering Terminology provides the standard definition of bugs: Inside a product, a bug is an error or a problem present in the process of software product development or maintenance; outside a product, a bug is a side effect or breach when the system is required to achieve a certain function.

2.1.2 Crack into software reversely

The code of the developer is the main cause of computer software defects owing to irregular and insecure programming. Several software developers give little or no consideration to software security issues during the design and preparation phase of the initial code, and thus, after the delivery of the software, inappropriate use by the user often easily leads to the generation of defects. In the present open architecture of computing systems, users have complete control over their systems and can modify the software and its associated processes. Some users will attempt to analyze the software protection mechanism, often with a malicious purpose. Software developers are usually required to prevent reverse engineering of the software to protect unauthorized copies of the software or intellectual property in the software. Commonly used encryption algorithms, such as advanced encryption standard (AES), Rivest-Shamir-Adleman (RSA) cryptosystem, and elliptic curve cryptography (ECC), are designed to exchange encrypted messages between "trusted" entities. The operations of encryption and decryption are performed safely inside a "black box" to avoid repetition. Attackers only exist between trusted entities, and cannot know the meaning of information and the concrete implementation of encryption and decryption entities. There are various code protection technologies in the market that prevent reverse engineering and code analysis. Regardless of their success and complexity, these technologies are unable to act against a common crack. The so-called universal crack refers to that if a software instance is cracked successfully, this cracking method can be applied to all instances of the same software subsequently. This undoubtedly causes a huge loss to software vendors. The fundamental reason is that all the copies of the target software have the same binary code such that the attacker can successfully develop a common cracking method.

2.2 Significance of solving software security issues

Based on the demand and with the intensification of various information leaks and numerous advanced persistent threat (APT) attacks, the awareness of the enterprises regarding information security has switched from "passive defense" to "active defense." In particular, the latest Internet financing, electricity businesses, and cloud computing consider forward-looking security as an important competitive force in the market and demand a variety of resources to enhance security.

The software industry with a large scale can not only raise the national economic index, but can also significantly improve the overall operational efficiency of national economy of the country. With further development of the information economy, the software industry will become a symbol of the overall national strength of a country. The software security industry, which is instrumental in protecting the development of the country, has a ripple effect on other industries. The significance of the development of the software security industry lies in the development of not only the software industry, but also the traditional manufacturing industry; the software security industry has a major stimulating effect on the entire social economy.

3 Solution of software security issues

3.1 Autonomous and controllable software

When considering software security, often only external security measures are considered, such as firewalls, intrusion detection systems, and anti-virus software; however, these security measures may be invalid for backdoor attacks and vulnerabilities. The essence of information security is autonomous and

controllable, so it is necessary to attach significant importance to the security issues of information systems, particularly, the basic hardware, software, and core equipment. The concept of autonomous and controllable software lays emphasis on the adoption of domestic software. Although it focuses on using products domestically, it also clarifies that this does not ensure safety. The uniqueness of information security is the existence of a "third party," i.e., a threat side that is not static. Furthermore, there is still some difference between China and the developed countries in the development of the software industry. In the IT field, as several key technologies and components are often dependent on foreign countries, the quality and efficiency of software developed by China still need to be further improved. Thus, achieving completely autonomous and controllable in software in China still requires significant effort.

3.2 Software diversity

Cohen pointed out in 1993 that the homogeneity of software can introduce a potential threat to the security of a computer. The attacker can easily attack all the computers that deployed the specific software by exploiting the software vulnerabilities. Software diversification indicates that multiple instances of the same software have different executable binary codes. It was first practically used in the fault-tolerant mechanism of some important areas. Using a variety of alternative versions of programs clearly results in higher reliability and security than employing a single version of program. With only minor variations in the implementation of the function, the differences between the multiple alternative versions of programs are transparent to end users, and these programs have the same function. As for the hackers, all the instances have the same function, but they have different binary codes and running processes. Software diversification prevents hackers from applying the information obtained from an instance to other instances. It also makes it difficult for them to develop generic exploitations and solutions that are applicable to all instances of the entire software. Thus, each software instance must be individually attacked or cracked. Software diversification is a very effective technique to deal with common attacks and cracks. It can strongly increase the difficulty and time required to crack protected application software. In extreme cases, an attacker will even have to perform a separate analysis on the binary code of each client side. Software diversification is very proficient at preventing attacks when the software is distributed and installed in an open environment. There are several ways to implement software diversification such as multi-version programming using different programming languages (C/JAVA/Python/Object-C), compiler-based software diversification, and software binary code rewriting.

Although, software diversification increases to a certain extent the threshold for the attacker to attack and crack software, it also increases the difficulty of software development and maintenance. On the one hand, software development needs high cost; on the other hand, software maintenance is more complex with the implementation of software diversification.

3.3 Mimic defense technology

Although software diversification increases the difficulty of utilizing a vulnerability for software attacks, it does not eliminate the threat. Therefore, to achieve higher security and reliability of the system, it is necessary to not only use a variety of different software versions, but also introduce a majority voting mechanism to produce a more reliable output compared with a single version of the program. In this case, the idea of mimic defense based on diversification (heterogeneity) of the voting mechanism, and the diversification can be applied to the software, hardware, and other components.

A software protection scheme based on mimic defense technology does not depend on its own confidentiality, since it constructs a set containing multiple heterogeneous variants for protected software via the software diversification method. This commonly used method utilizes a diverse compilation to generate a set of variants. Compiler-based diversification techniques, such as equivalent instruction substitution, control flow obfuscation, and insertion of junk codes, modify the object code of programs by different degrees, add new extraneous instructions, or change the direction of existing control flow. Fig. 1 shows the generation process of functionally equivalent multiple variants, which relies on a diversified compiler. All input to a program is copied and distributed to all heterogeneous variants. The heterogeneous nature of the multiple variants is related to the diversified techniques employed. When the attack characteristic coincides with the heterogeneity of the variant, the output of the attack is different for different variants. By comparing all the outputs of the variants and voting on them, an attack aiming at heterogeneous features can be defend, and thus, the attacked variant can be identified. The detailed design framework is shown in Fig. 2 and variants A, B, and C are generated by a diverse compiler within the same software source code.

From the designed framework based on the mimic defense technology, it is evident that the input of a program must be given to the three variants simultaneously. The advantages of this framework are as follows.

(1) It uses a variety of security mechanisms to disrupt or block the attack chain and increase the difficulty of the attack;

(2) It allows the use of "poisonous or bacteria-bearing" software components and can control the security risk;

(3) A combination of software operating mechanisms can constitute a considerable dynamic space to effectively reduce the reliability of exploiting vulnerabilities and backdoors to attack;

(4) High availability of redundant and inherently redundant mimic architecture renders the mimic security defense system inherently reliable;

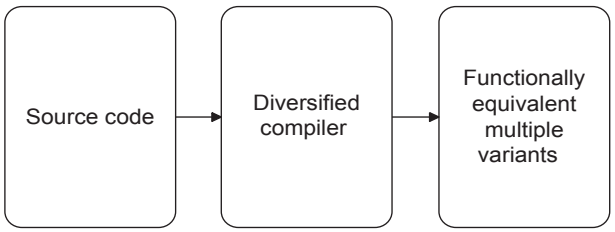

Fig. 1. Generation process of functionally equivalent multiple variants.

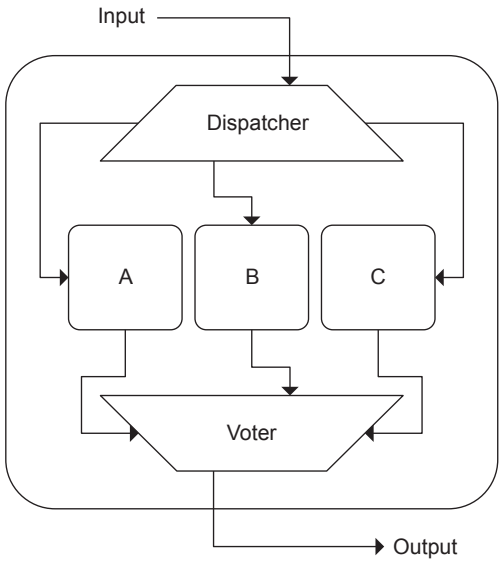

Fig. 2. Designed framework based on the mimic defense technology.

(5) It can form special operating mechanisms such as symbiotic synergy, *N* variants, equivalent variants, and heterogeneous environmental migration to provide innovative methods for "poisons-tolerant" operations and for timely detection, suppression, blocking, and removal of Trojans and viruses.

4 Conclusions

In the background of cyberspace security and globalization, industrial cooperation and competition between countries is becoming steadily intense. The software industry not only has significant development opportunities and challenges, but also faces increasingly complex security issues. The solution to the issues of software security not only needs the existing security technologies, but also needs the theoretical innovation guidance and technical support. The development of a new generation of software systems must cooperate with the national security strategy. On the one hand, the research and development of a software system with independent controllability should be focused; on the other hand, the security architecture of mimic defense to realize a trusted system based on non-trusted components should also be utilized to achieve software security in all aspects.

As a "rebalancing strategy of cyberspace," mimic defense technology, an important aspect of software security architecture, can address software security vulnerabilities that can be attacked and cracked. Within the asymmetry of the current market share of the software security industry and in view of the differences in the security status at domestic and international levels, a mimic defense technology provides a new way to solve the problem of component-level security. Thus, the security architecture technology can defend against software vulnerabilities and backdoor attacks, particularly unknown ones, and can alleviate the software security threats introduced by technical weaknesses. Moreover, the mimic defense technology is one of the first proposed active defense technologies. The technology itself is autonomous and controllable for the security issues of the software industry, and it provides a universal solution for the information system software security issues.

References

[1] China Internet Network Information Center. The 38th statistical report on Internet development in China [EB/OL]. (2016-08-03) [2016-10-08]. http://www.cnnic.net.cn/hlwfzyj/hlwxzbg/hlwtjbg/201608/t20160803_54392.htm. Chinese.

[2] Symantec Corporation. Internet security threat report 2016 [R/OL]. (2016-04-01) [2016-10-08]. https://www.symantec.com/content/dam/symantec/docs/reports/istr-21-2016-en.pdf.

[3] Ni G N. The nature of information security: autonomous and controllable [J]. China Economy & Informatization, 2013 (5): 18–19. Chinese.

[4] Cohen F B. Operating system protection through program evolution [J]. Computers & Security, 1993, 12 (6): 565–584.

[5] Wu J X. Meaning and vision of mimic computing and mimic security defense [J]. Telecommunications Science, 2014, 30 (7): 1–7. Chinese.

[6] Jackson T, Salamat B, Homescu A, et al. Compiler-generated software diversity [M]// Jajodia S, Ghosh A K, Swarup V, et al, editors. Moving target defense: creating asymmetric uncertainty for cyber threats. New York: Springer, 2011: 77–98.

[7] Wu J X. Mimic security defense in cyber space [J]. Secrecy Science and Technology, 2014, 10 (1): 4–9. Chinese.