Code 004.056

ABOUT ONE APPROACH TO DETECTING COMPUTER THREATS

Beridze Besik

Batumi Shota Rustaveli State University

Abstract

This paper considers several specific methods for detecting an attack on an information system based on the approach of fixing the system's anomalous behavior.

Through these examples, the author confirms the validity of this approach and gives directions for the further development of security methods based on this approach.

Аннотация

Рассматривается несколько конкретных методов обнаружения атаки на информационную систему, основанных на подходе фиксации аномального поведения системы.

Через эти примеры автор подтверждает действенность данного подхода и приводит направления для дальнейшего развития методов обеспечения безопасности, на основании этого подхода.

Introduction

The modern world cannot be imagined without communication and computing. The fast development of information technologies has a serious impact on all patterns of human activity. Therefore, it is clear that the security of information technology has become a prerequisite for society's normal existence.

The development of information technology has created a new type of crime: cybercrime. Among the systems in which cyber attacks are carried out, the banking and financial systems are the primarily targets. Automated management systems for educational institutions are a close second in terms of "attention" from attackers. Every day, there are new methods of attacking computer systems based on practical analysis—programs that encrypt network traffic, with which we can find information such as users or their password identifiers, bank accounts, and much more. It is clear that if society cannot effectively counter cyber threats, it will be forced to abandon some advantages of information technologies since their use will lose all meaning. It is thus clear how important it is to develop tools and methodologies for cybersecurity.

Experiments and research in the field of cybersecurity, in which the whole world participates, are not a single approach today, it is necessary to organize knowledge and create a common structure [1,2].

Unlike other methods, the approach that needs to be discussed, ideally, will allow us to identify the danger by developing separate stages of various attacks, while they are still in the process of preparation and formation, and not at the stage of implementation.

Use information about expected hazards:

The method under consideration determines the likelihood of a specific hazard to identify the vulnerability of a given system based on subjective analysis. This approach is suitable for systems whose behavior in "quiet" conditions is easily obeyed by certain rules and is easily predictable. Under such conditions, it is relatively easy to identify and respond to a "problem" (source/cause of abnormal behavior) in the system. The dangers of an information system are usually interconnected. For example, the presence of an incorrect, weak web server can lead to a criminal mastering the entire data node, therefore, it is necessary to anticipate the possibility of a probable connection between the threats to predict and assess the situation.

If you allow U to be a space of security threats that can be examined by an information system, then the user interface will have certain threats for compiling the U space. The implementation of the first threat will most likely lead to the implementation of other threats. At this time, it is necessary to calculate P (u | u1, u2, ..., uk), the probability of realization of the threat U will be equal to u | u1, u2, ..., uk performance [3,4].

A more error-free attack can be detected if we have complete information about the event. The essence of the attack detection concept is to classify expected attacks. Classification issues are still being actively studied [5].

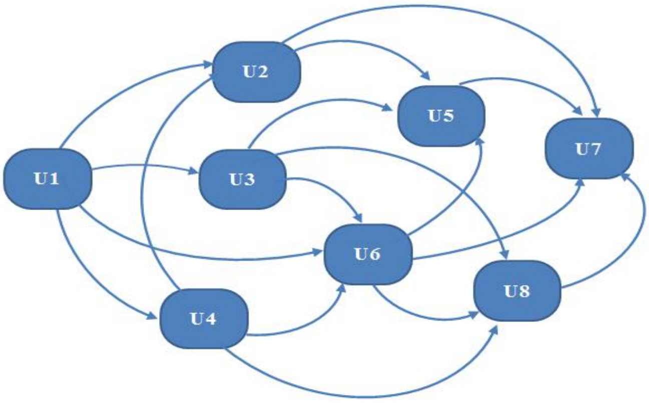

Figure.1 – A graphical representation of the probabilistic relationship between threats

Analysis of the correlation of threats associated with the phases of an attack and predicting the most likely threat that may arise during an attack is an important task in ensuring information security.

Technologies of redistributed anomalies:

Sensors detect the activation of unnatural (suspicious) actions when they notice that access to the system is not legally permitted. For more detailed information, I propose these specific protection methods that I developed:

If the “NIS error” is corrected, the system perceives this as abnormal behavior and automatically disables authorization for Guest users; the system predicts that the attackers will try to access the system with administrator rights using a guest user, and sends a message to the administrator about the incident.

An attempt by attackers to enter the system in an unauthorized manner ("system concern") is perceived by the ADS (attack detection system) as abnormal behavior because it is recorded as an unsuccessful attempt to enter. If a high number of attempts are detected, ADS reserves the right to change the file structure of the system and at the same time sends a message to the administrator about the incident.

ADS also observes the system and user files in particular and fixes whether a new file is created by the user registered in the system, observes the CPU load size, memory buffer size, and the case when an attacker’s unauthorized access copies the system file. Since the size of the memory and the buffer has changed but the number of files is unchanged, the workload of the processor is observed to be a high percentage of the load. In response, the system shuts down the port so that information does not leak and sends a message to the administrator about the incident.

Conclusion

Specific examples of attack detection based on the approach of searching for anomalies in the behavior of the system demonstrate the effectiveness of this approach. In the future, it is advisable to develop other specific solutions based on this approach, as well as to explore the possible combination of this approach with other approaches.

A separate study is worthwhile to develop a methodology for building better technological systems for this approach.

References

1.Robert Newman, Computer Security: Protecting Digital Resources. 2010

2.John R. Vacca, Network and System Security. 2014

3.Christos Douligeris, Dimitrios N. Serpanos, Network Security: Current Status and Future Directions 2007

4.John R. Vacca, Managing Information Security. 2010

5.A.V. Arganovski, P.A. Khadi, Computer Threat Detection Systems: http://www.nestor.minsk.by/sr/2008/05/sr80513.html Source - 20.04.2020