HONORS GROUP

IN

THE 31st ANNUAL

Science Talent Search®

for the

Westinghouse Science Scholarships

and Awards

1972

SCIENCE CLUBS OF AMERICA
Administered By Science Service
1719 N STREET N.W. WASHINGTON, D. C. 20036
The Annual Science Talent Search

The Meaning of Honors in the Science Talent Search

FOR RELEASE: WEDNESDAY AFTERNOON, JANUARY 26, 1972

Honors Group
Useful references:


Bengaluru, India

Indian Institute of Science

Department of Computer Science and Automation

2000

Anshul Agrawal, Chinmoy Dasgupta, and Janakiram Sivaramakrishnan

Computer Science and Automation

Indian Institute of Science

Bangalore 560012, India

Phone: +91 80 2293 3940 (ext. 237)
Email: cs@iisc.ernet.in

Abstract

In this paper, we present a new approach to the problem of detecting and removing ad-hoc malicious code from software systems. Our approach is based on the idea of using a combination of static analysis and dynamic analysis techniques to identify and remove malicious code. We describe the design and implementation of our system, and present experimental results that demonstrate the effectiveness of our approach.

Keywords

Malicious code detection, static analysis, dynamic analysis, software security, ad-hoc malware.

1. Introduction

In recent years, there has been an increasing number of reports of ad-hoc malicious code being used to attack software systems. This type of malware is difficult to detect and remove, as it is not typically distributed through official channels and is not subject to the same level of scrutiny as more conventional malware.

2. Related Work

There has been a great deal of research into the problem of detecting and removing malicious code from software systems. Most existing approaches focus on static analysis techniques, which involve analyzing the source or binary code of a program in order to identify potential security vulnerabilities.

3. Our Approach

Our approach to detecting and removing ad-hoc malicious code is based on the idea of using a combination of static and dynamic analysis techniques. Static analysis is used to identify potential security vulnerabilities, while dynamic analysis is used to actually remove the malicious code from the software system.

4. System Design

Our system consists of two main components: a static analysis component and a dynamic analysis component. The static analysis component is used to identify potential security vulnerabilities in the software system, while the dynamic analysis component is used to actually remove the malicious code from the system.

5. Experimental Results

We have conducted a number of experiments to evaluate the effectiveness of our system. Our results show that our approach is able to accurately detect and remove ad-hoc malicious code from software systems.

6. Conclusion

In conclusion, we have presented a new approach to the problem of detecting and removing ad-hoc malicious code from software systems. Our approach is based on the idea of using a combination of static and dynamic analysis techniques, and we have demonstrated the effectiveness of our approach through a series of experiments.

References


Acknowledgments

This work was supported in part by the Indian National Science Academy (INSAS) and the Department of Science and Technology (DST), Government of India.