Abstract

Computer hardware and Internet is growing so fast today, security threats of malicious executable code are getting more serious. Basically, malicious executable codes are categorized into three kinds – virus, Spam, Trojan horse, and worm. Current anti-virus products cannot detect all the malicious codes, especially for those unseen, polymorphism malicious
executable codes[1]. The newly developed virus will create the damages before it has been found and updated in database. Spy ware is becoming a real concern [2]. The proposed architecture classifies the behavior of the new type virus and it identifies the malicious code through the virtual server, where all the unwanted code executions and dependable are get refined first before it reaches the actual server. This phenomenon is known as virtual engineering. The security features in the virtual server get processed virtually through reverse engineering technique [3]. Here the user or the administrator checks the application first automatically in the virtual server and it analyze the behavior and filters the malicious code and protects the actual server, this process is very fast compare to other architecture which we have noticed in emerging operating systems.

Reference

- Bright Hub available at www.brighthub.com
- Info Security available at www.infosecurity-us.com
- Computer Security Training, Network Research & Resources available at www.sans.org
- PHYSORG available at www.physorg.com
- TalkTechToMe available at www.gfi.com/blog/tag/patch-management
- HACKER BOSS available at www.hackerboss.com
- Web Application Vulnerabilities available at www.acunetix.com/vulnerabilities
- guardian.co.uk available at www.guardian.co.uk/2011/google-android-patent-lawsuits-batt.
- Peter Braun, Manfred Broy, Frank Houdek, Matthias Kirchmayr and Mark Müller, et al. Online First™, 20 October 2010
- Securing SQL Server available at www.securingsqlserver.com/tag/sql-injection
- Performance comparison and analysis of mobile ad hoc routing protocols: An International Journal (CSEIJ), Vol.1, No.1, April 2011

Index Terms

Computer Science
Security
Key words

Function Extraction Technology Malicious code
Patching
Reverse Engineering
Security threats
Virtual Engineering