

## A MINING METHOD FOR COMPUTER VULNERABILITY CORRELATION

YONG-ZHENG ZHANG

National Computer Information Content Security Key Laboratory  
Harbin Institute of Technology  
P.O. Box 320, No. 92, West Da-Zhi Street, Harbin 150001, China  
zyz@pact518.hit.edu.cn

XIAO-CHUN YUN, BIN-XING FANG

Research Center of Computer Network and Information Security Technology  
Harbin Institute of Technology  
P.O. Box 320, No. 92, West Da-Zhi Street, Harbin 150001, China  
yxc@hit.edu.cn; bxfang@pact518.hit.edu.cn

TAO ZHANG

National Computer Information Content Security Key Laboratory  
Harbin Institute of Technology  
P.O. Box 320, No. 92, West Da-Zhi Street, Harbin 150001, China  
zhangtao@pact518.hit.edu.cn

Received July 2004; revised December 2004

**ABSTRACT.** *With the development of computer software system, computer vulnerabilities are continually increasing. These vulnerabilities have severe impacts on confidentiality, authenticity and availability of computer system and network. In the field of host system vulnerability assessment, the traditional method is only to consider the threats of isolated vulnerability to software systems. However, through analyzing multistage attacks and vulnerabilities on Internet, we find that attackers often synthetically exploit several correlative vulnerabilities to badly compromise the systems. Therefore, study on vulnerability correlation is important for improving the accuracy and validity of security assessment. This paper firstly gives the definition, expression and significance of vulnerability correlation. Then a mining method for vulnerability correlation is proposed. Finally, an experiment is conducted to verify the efficiency of the new approach.*

**Keywords:** Security assessment, Computer vulnerability, Vulnerability correlation, Mining method

**1. Introduction.** With the development of computer software system, computer vulnerabilities are continually increasing. These vulnerabilities are mainly derived from Social engineering, Logic error, Policy oversight and Weakness [1]. They have severe impacts on confidentiality, authenticity [2] and availability of computer system and network. Currently, many scientific organizations and researchers are engaged in vulnerability analysis

---

This work is supported by the "Tenth Five-Year Plan" of Chinese National Defense Pre-research Program under grant No. 4131571.